Exhibit 16

WSP Manual

Alpine Securities Corporation

August 29th, 2014

TABLE OF CONTENTS

misappropriation of funds, or securities, or a conspiracy to commit any of these offenses, or substantially equivalent activity in a domestic, military or foreign court;

- is a director, controlling stockholder, partner, officer or sole proprietor of, or an associated person with, a broker, dealer, investment company, investment advisor, underwriter or insurance company that was suspended, expelled or had its registration denied or revoked by any domestic or foreign regulatory body, jurisdiction or organization or is associated in such a capacity with a bank, trust company or other financial institution that was convicted of or pleaded no contest to, any felony or misdemeanor in a domestic or foreign court;
- is a defendant or respondent in any securities- or commodities-related civil litigation or arbitration, is a defendant or respondent in any financial-related insurance civil litigation or arbitration, or is the subject of any claim for damages by a customer, broker or dealer that relates to the provision of financial services or relates to a financial transaction, and such civil litigation, arbitration or claim for damages has been disposed of by judgment, award or settlement for an amount exceeding $15,000. However, when the member is the defendant or respondent or is the subject of any claim for damages by a customer, broker or dealer, then the reporting to FINRA shall be required only when such judgment, award or settlement is for an amount exceeding $25,000; or
- is, or is involved in the sale of any financial instrument, the provision of any investment advice or the financing of any such activities with any person who is, subject to a "statutory disqualification" as that term is defined in the Exchange Act. The report shall include the name of the person subject to the statutory disqualification and details concerning the disqualification; or

2. an associated person of the member is the subject of any disciplinary action taken by the member involving suspension, termination, the withholding of compensation or of any other remuneration in excess of $2,500, the imposition of fines in excess of $2,500 or is otherwise disciplined in any manner that would have a significant limitation on the individual's activities on a temporary or permanent basis.

3.14 Money Laundering

[FINRA Rule 3310; Bank Secrecy Act]

This section provides a brief overview of the employee's responsibilities concerning the prevention and detection of money laundering. Please refer to the chapter titled "*Anti-Money Laundering (AML) Program*" for more detailed information about Alpine's AML Program.

3.14.1 Reports Of AML Non-Compliance And Other Potential Crimes

All employees are obligated to promptly report to the AML Compliance Officer or designee any known or suspected violations of anti-money laundering policies as well as other suspected violations or crimes. If the potential violation implicates the AML Officer, it should be reported to a senior officer of Alpine. All reports are confidential and the employee will suffer no retaliation for making them.

What to report: Crimes or suspected crimes by individuals (whether associated with Alpine, a customer, or prospective customer) are required to be reported. This includes suspicion that Alpine is being used as a conduit for criminal activity such as money laundering or structuring transactions (discussed below) to evade the Bank Secrecy Act reporting requirements. There is no clear definition of what constitutes a "crime." If you believe some improper or illegal activity is occurring, it is your obligation to be attentive and alert to the red flags and report to the AML Compliance Officer or designee any new or existing customers who may be engaged in violations of anti-money laundering regulations.

SAR reports: By law, Alpine and its employees cannot disclose to the customer or anyone other than authorized parties that it has filed a SAR or provide information that would reveal the existence of a SAR. Questions regarding SAR filings should be referred to Compliance. If you become aware of an unauthorized disclosure of an SAR or you receive a subpoena for an SAR, **immediately contact the Compliance Department**. Designated Compliance personnel will be responsible for contacting FINCEN to report the unauthorized disclosure.

3.14.2 Identity Theft

Identity thieves use someone's personal identifying information to open new accounts and misuse existing accounts. Alpine has established an Identity Theft Prevention Program (ITPP) to help detect and prevent identity theft. Many elements of detecting or preventing identity theft utilize similar techniques to that of the anti-money laundering (AML) requirements included within these policies.

The ITPP is based on identifying "red flags" which may indicate an occurrence of identity theft. ***It is the responsibility of all employees to be attentive and alert to the red flags and report to the AML Compliance Officer any new or existing customers who may be engaged in violations of anti-money laundering regulations, identity theft or who have reported an instance of identity theft.***

For a list of potential identity theft red flags, refer to the section titled "*Red Flag Identification and Detection Grid*" located in the ***Identity Theft Prevention Program (FTC Fact Act Red Flags Rule)*** section.

3.15 Emergency Business Recovery Procedures

[FINRA Rule 4370]

Alpine has a *Business Continuity Plan* ("BCP") that assigns responsibilities and outlines procedures in the event of a disaster, emergency or pandemic which impacts the ability of Alpine to continue conducting business (also termed a "significant business disruption"). Examples of a significant business disruption include a regional power outage; disruption at another company that provides services critical to Alpine; and destruction of an office or other facilities by natural causes or by other means. The BCP designates employees who are responsible for employee safety and protection of firm property, records, and customer assets.

In the event of a disruption, employees will be given instructions by authorized personnel. Depending on the nature of the emergency, it may be necessary to use alternate communication systems; transfer personnel and/or business activities to alternate office space; or transfer Alpine's business to other brokerage firms or financial institutions until normal operations can be resumed.

Alpine has established procedures for contacting employees in the event of an emergency. If Alpine conducts a test of its emergency procedures, all employees are required to participate as if the emergency were real. Past emergencies affecting the securities industry have shown that preparedness and cooperation are key to maximizing the safety of employees and minimizing business interruptions. It is important for all employees to follow instructions from senior management and other authorized key personnel during any drill or when an emergency occurs.

Questions regarding Alpine's Business Continuity Plan may be referred to the Chief Operating Officer.

Responsibility	• COO
Resources	• Business Continuity Records
Frequency	• Annually or as required
Action	• Administer the Business Continuity Plan • Perform annual tests for compliance with the policy
Record	• Copies of Alpine's business continuity plan • Copies of dates in which the plan is tested

	devices used to access firm and customer data • Require encryption of data on laptops and other mobile devices • Limit access to customer information to employees who have a reason to see it • Monitor on an ongoing basis for breaches including review of web server logs to reveal intrusions • When system intrusions are detected, follow protocol for compromised data • Conduct due diligence/obtain affirmation from third parties with access to firm data • Issue passwords to authorized personnel including use of strong passwords through validation or periodic password changes and forced password expiration; disable them when an authorized person terminates or transfers from an authorized position, including shared user names and passwords when one of the users terminates or is no longer an authorized person • Provide training to personnel (may be part of annual compliance or other meetings, or media) including: keeping customer information secure and confidential; limitations on use of computers, software, access to accounts; locking and securing mobile devices when not in use; customer breaches: identifying, reporting to CCO or designee • Test systems regularly and correct anomalies • Conduct periodic audits and review of internal controls and procedures (Compliance or other assigned personnel) including audits of employee computers to confirm installation of security software and use of encryption; follow up regarding audit findings (internal or external)

Alpine's IT Committee is responsible for developing and implementing procedures to protect Alpine's internal systems and data.

8.36 Correspondent Clearing

More information about Alpine Securities' correspondent clearing business policies and procedures can be found in the Chapter titled "Correspondent Clearing/Due Diligence for Correspondent Firms located elsewhere in this Manual.

9 ANTI-MONEY LAUNDERING (AML) PROGRAM

9.1 Firm Policy

Alpine revised this policy, which became effective on June 30th, 2014.

It is the policy of Alpine Securities Corporation (Alpine) to prohibit and actively prevent money laundering and any activities that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the Bank Secrecy Act (BSA) and its implementing regulations.

Money laundering is a serious crime potentially related to the funding of terrorist activities. It is the subject of extensive federal regulations that impose requirements on financial institutions, such as broker-dealers and their employees, to detect and prevent potential money laundering activities. Actions to detect and prevent money laundering is an obligation of each Alpine employee.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activity is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate

the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal or legitimate business activities.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Engaging in money laundering and terrorist financing is a federal crime with severe penalties for those engaged in the associated criminal activities and those who facilitate, intentionally or inadvertently, money laundering. It is important that Alpine and all employees, remain diligent and active participants in Alpine's Anti-Money Laundering (AML) Program.

This chapter explains Alpine's Anti-Money Laundering (AML) Program. An explanation of money laundering and guidance for all employees to detect money laundering is included in this chapter. These policies will be updated and appropriate procedures and action effected when new rules are adopted.

9.1.1 Background

The Currency and Foreign Transactions Reporting Act, also known as the Bank Secrecy Act (BSA), and its accompanying regulation, is a tool the U.S. government uses to fight drug trafficking, money laundering, and other crimes. Congress enacted the BSA to prevent financial service providers (such as banks and broker-dealers) from being used as intermediaries for, or to hide the transfer or deposit of, money derived from criminal activity. Money laundering schemes may include the use of wire transfers, cash, bearer instruments, travelers' checks, money orders, cashiers' checks, and other negotiable instruments.

Alpine is required to comply with the reporting, recordkeeping, and record retention requirements of the BSA. The requirements govern the payment, receipt, or transfer of currency within, into and out of the U.S. and foreign financial transactions and accounts.

9.2 AML Officer Designation and Duties

[NASD Rule 1160; FINRA Rule 3310(d) and 3310.02]

Rules/Resources: FINRA Rule 3310; Bank Secrecy Act, 31 C.F.R. 103.120(c)

Alpine has designated an AML Officer who is responsible for overseeing Alpine's anti-money laundering program, developing policies, procedures, and internal controls reasonably designed to achieve compliance with AML rules and regulations. Please refer to Alpine's Form BD for the contact name of the AML Officer. The AML Officer has a working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge and training. The duties of the AML Officer or designee will also include monitoring the firm's compliance with AML obligations and overseeing communication and training for employees. The AML Officer or designee will also ensure that suspicious activity reports (SAR-SFs) are filed with the Financial Crimes Enforcement Network (FinCEN) when appropriate.

Contact the AML Officer or designee whenever you have questions about Alpine's program, a current or prospective account, or activities or transactions that raise questions about potential money laundering or other illicit activities. You may also provide information anonymously to the AML Officer or designee. The AML Officer or designee is responsible for investigating suspected money laundering activities and taking corrective action when necessary.

9.3 Updates to the FINRA Contact System

Rules/Resources: 31 C.F.R. § 103.120; FINRA Rule 3310, NASD Rule 1160.

Responsibility	• CCO or designee
Resources	• FINRA Contact System
Frequency	• As required as material information becomes inaccurate; and • Annual confirmations within 17 business days following the end of the calendar year
Action	• Provide AML Officer name and contact information to FINRA via the FINRA Contact System (FCS), initially • Notify FINRA promptly of any material changes in the AML Officer's contact information for the AML Officer within 30 days following the change. • Confirm information via FINRA Contact System (FCS) annually within 17 business days following the end of the calendar year
Record	• Updates via FINRA Contacts System (through FINRA Gateway)

Alpine will provide FINRA with contact information for the AML Officer, including: (1) name; (2) title; (3) mailing address; (4) email address; (5) telephone number; and (6) facsimile number through the FINRA Contact System (FCS) within 30 days following the material change. The CCO or designee will promptly notify FINRA of any material change in this information through FCS and will review, on an annual basis and if necessary update, this information within 17 business days after the end of each calendar year.

9.4 General Summary of AML Officer Duties

Rules/Resources: NASD Rule 1160; FINRA Rule 3310(d) and 3310.02

Responsibility	• AML Officer or designee
Resources	• Computer reports and other programs developed for the Program • Internal audits or outside audits of the Program • Regulations and rules for broker-dealer anti-money laundering programs • OFAC web site • Other sites and resources available
Frequency	• Annual - review policies and procedures • Annual and more frequently, as needed - develop and schedule AML education for employees • As needed - update program and provide revisions to senior management for review and approval of material changes. Non-material changes to the AML Policy will not require senior management approval. • Annually - review AML contact information on file through the FINRA Contact System (FCS) • Ongoing - review new regulations • Ongoing - monitor activity
Action	• Develop and update Alpine's anti-money laundering program

	• Obtain senior management approval for any material changes to the program or policy • Monitor (or designate monitoring) the activity of Alpine, its associated persons, and customers to reasonably detect and prevent money laundering activities • Develop AML education program for employees and schedule training • File required reports • Retain required records • Provide contact information via the FINRA Contact System (FCS) and update contact information if necessary
Record	• Designation of AML Officer • Retain current and past copies of anti-money laundering program with senior management approval, when and where senior management approval is required • Retain records of AML education including who attended, date of training, and material covered • Reports filed along with supporting documentation, where applicable • Retain other records, as listed in the Program

9.5 Giving AML Information to Federal Law Enforcement Agencies and Other Financial Institutions

9.5.1 Requests and Written Notices From Enforcement Agencies

Under the Bank Secrecy Act, financial institutions are required to respond to federal banking agency requests for information relating to anti-money laundering compliance. The Rule requires provision of information and account documentation for any account opened, maintained, administered or managed in the U.S. The AML Officer or designee maintains records of information provided in response to regulators' requests including the request, date of response, and information provided.

9.5.2 Federal Banking Agency Requests - 120 Hour Rule

Rules/Resources: USA PATRIOT Act Section 319(b)

Upon receiving a request from a Federal banking agency, the AML Officer or designee will provide the requested information within 5 days (120 hours) of receiving the request or will make available the information for inspection by the banking agency.

9.5.3 FinCEN Requests Under USA PATRIOT Act Section 314(a)

Rules/Resources: Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart E; USA PATRIOT Act Section 314; FinCEN 314(a) Fact Sheet: http://www.fincen.gov/statutes_regs/patriot/pdf/314afactsheet.pdf, *31 C.F.R. 103.100.*

Resources:FinCEN press release (2/6/03);FinCEN press release (2/12/03);NASD Member Alert (2/14/03);FinCEN's 314(a) Fact Sheet (11/18/08), Frequently Asked Questions (FAQs)

Responsibility	• AML Officer or designee
Resources	• Deposit records, purchase/sale records, account records, other records as required

Frequency	• Upon request
Action	• Conduct a search of the required records • If a match is found, submit the Subject Information Form to FinCEN using the Secure Information Sharing System • Retain copy of 314(a) list received
Record	• Retain copies of the request • Notate date of review and initial or sign the 314(a) list received • Information submitted (if a match is found) are retained in a FinCEN information request file • Sign or initial 314(a) Search Self-Verification Page and retain

The Financial Crimes Enforcement Network (FinCEN) sends law enforcement requests to financial institutions under Section 314(a) of the USA PATRIOT Act, on typically, a bi-weekly basis.

Alpine will respond to a Financial Crimes Enforcement Network (FinCEN) 314(a) Request concerning accounts and transactions by immediately searching our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity or organization named in the 314(a) Request as outlined in the Frequently Asked Questions (FAQ) located on FinCEN's secure Web site. Alpine understands that we have 14 days (unless otherwise specified by FinCEN) from the transmission date of the request to respond to a 314(a) Request. If the search parameters differ from those mentioned above (for example, if FinCEN limits the search to a geographic location), the AML Officer or designee will structure the search accordingly. Unless otherwise stated in the 314(a) Request or specified by FinCEN, Alpine is required to search those documents outlined in FinCEN's FAQ . If Alpine finds a match, the AML Officer or designee will report it to FinCEN using FinCEN's Secure Information Sharing System. If we find a match with a named subject, the AML Officer or designee can stop its search on that subject; as we are not required to search our records further for other matches with that specific subject unless and until we have been contacted by the requesting federal law enforcement agency for additional information. If the 314(a) Request contains multiple subjects, the AML Officer or designee will continue to search our records for an account or transaction matching any of the other named subjects. The AML Officer or designee will ensure that all searches have been completed prior to reporting any matches, as we will not be able to submit the response more than once for any review period. The AML Officer or designee should not send any record of an account or a transaction (other than a report, as described above, notifying FinCEN of a match) when responding to a 314(a) Request.

If the AML Officer or designee searches Alpine's records and does not find a matching account or transaction, then the AML Officer or designee will not reply to the 314(a) Request. Alpine will maintain documentation that we have performed the required search by following the processes outlined above.

Alpine will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. The AML Officer or designee will review, maintain and implement procedures to protect the security and confidentiality of requests from FinCEN similar to those procedures established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act with regard to the protection of customers' nonpublic information.

Unless otherwise stated in the 314(a) Request, Alpine will not be required to treat the information request as continuing in nature, and Alpine will not be required to treat the periodic 314(a) Requests as a government provided list of suspected terrorists for purposes of the customer identification and verification requirements.

9.5.4 National Security Letters

Rules/Resources: FinCEN SAR Activity Review, Trends, Tips & Issues, Issue 8 (National Security Letters and Suspicious Activity Reporting) (4/2005).

National Security Letters (NSLs) are written investigative demands that may be issued by the local Federal Bureau of Investigation and other federal government authorities conducting counterintelligence and counterterrorism investigations to obtain, among other things, financial records of broker-dealers. NSLs are highly confidential. No broker-dealer, officer, employee or agent of the broker-dealer can disclose to any person that a government authority or the FBI has sought or obtained access to records. Alpine has policies in place to process and maintain the confidentiality of NSLs. If we file a Suspicious Activity Report (SAR-SF) after receiving a NSL, the SAR-SF should not contain any reference to the receipt or existence of the NSL.

9.5.5 Grand Jury Subpoenas

Resources: FinCEN SAR Activity Review, Trends, Tips & Issues, Issue 10 (Grand Jury Subpoenas and Suspicious Activity Reporting) (5/2006).

Alpine understands that the receipt of a grand jury subpoena concerning a customer does not in itself require that we file a Suspicious Activity Report (SAR-SF). Alpine further understand that none of our officers, employees or agents may directly or indirectly disclose to the person who is the subject of the subpoena its existence, its contents or the information we used to respond to it. To maintain the confidentiality of any grand jury subpoena we receive, Alpine will process and maintain the subpoena in accordance with our departmental policies and procedures. If Alpine files a SAR-SF after receiving a grand jury subpoena, the SAR-SF will not contain any reference to the receipt or existence of the subpoena. The SAR-SF will only contain detailed information about the facts and circumstances of the detected suspicious activity.

9.5.6 Voluntary Information Sharing with Other Financial Institutions Under USA PATRIOT Act Section 314(b)

9.5.6.1 Information Sharing Between Financial Institutions

Rules/Resources: USA PATRIOT Act Section 314(b); Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart E; FinCEN certification: http://www.fincen.gov/fi_infoappb.html, Rule: 31 C.F.R. § 103.110., FinCEN Financial Institution Notification Form; FIN-2009-G002: Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act (06/16/2009).

Alpine will share information with other financial institutions regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering. The AML Officer or designee will ensure that the firm files with FinCEN an initial notice before any sharing occurs and annual notices thereafter. Alpine will use the notice form found at FinCEN's Web site. Before Alpine shares information with another financial institution, Alpine will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available. Alpine understands that this requirement applies even to financial institutions with which we are affiliated and that Alpine will obtain the requisite notices from affiliates and follow all required procedures.

Alpine will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, for example, by segregating it from the firm's other books and records.

Alpine also will employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

- Identifying and, where appropriate, reporting on money laundering or terrorist activities;
- Determining whether to establish or maintain an account, or to engage in a transaction; or

- Assisting the financial institution in complying with performing such activities.

9.5.6.2 Joint Filing of SARS by Broker-Dealers and Other Financial Institutions

Rules/Resources: 31 C.F.R. §103.19; 31 C.F.R. § 103.38; 31 C.F.R. § 103.110.

Alpine may file joint SARs in certain circumstances. Alpine may share information about a particular suspicious transaction with any broker-dealer, as appropriate, involved in that particular transaction for purposes of determining whether we will file jointly a SAR-SF.

If Alpine determines it is appropriate to jointly file a SAR-SF, Alpine understands that we cannot disclose that we have filed a SAR-SF to any financial institution except the financial institution that is filing jointly. If Alpine determine it is not appropriate to file jointly (*e.g.*, because the SAR-SF concerns the other broker-dealer or one of its employees), Alpine understands that we cannot disclose that we have filed a SAR-SF to any other financial institution.

9.5.6.3 Sharing SAR-SFs with Parent Companies

Rules/Resources: FinCEN Guidance on Sharing of Suspicious Activity Reports by Securities Broker-Dealers, Futures Commission Merchants, and Introducing Brokers in Commodities (1/20/06).

Because Alpine is a subsidiary, Alpine may share SAR-SFs with its parent company, if the financial institution has filed a current 314(b) information sharing form with FinCEN. Before Alpine shares SAR-SFs with our parent company, Alpine will have in place written confidentiality agreements or written arrangements that Alpine's parent company protects the confidentiality of the SAR-SFs through appropriate internal controls.

9.6 Checking the Office of Foreign Assets Control (OFAC) Listings

Rules/Resources: Dept. of Treasury, various statutes; OFAC web site (http://www.treas.gov/offices/enforcement/ofac/); Foreign Assets Control Regulations For The Securities Industry (http://www.treas.gov/offices/enforcement/ofac/regulations/t11facsc.pdf),SEC AML Source Tool, Item 12; OFAC Lists Web page (including links to the SDN List and lists of sanctioned countries); FINRA's OFAC Search Tool. You can also subscribe to receive updates on the OFAC Subscription Web page. See also the following OFAC forms: Blocked Properties Reporting Form; Voluntary Form for Reporting Blocked Transactions; Voluntary Form for Reporting Rejected Transactions; OFAC Guidance Regarding Foreign Assets Control Regulations for the Securities Industry.

Responsibility	• RR for a new account • OSJ Branch Manager and/or President or their designees ("Designated Supervisor(s)") • AML Officer or designee, where designated
Resources	• Name / Entity search based on above referenced OFAC web site • Comparison search program provided by CSS Hosted Solutions, LLC, (hereafter referred to as the OFAC screening report) • Other sites identified below (such as *www.treas.gov/ofac* or *www.fincen.gov*
Frequency	• At the time that a new account is opened • Daily for the OFAC screening report o Weekly for the following reports: ▪ Account Activity in Non-Cooperative and Blocked Countries Report ▪ Account in Non-Cooperative Countries Report

	▪ Foreign Account Activity Report
Action	• RR shall perform an OFAC search for each new customer and attach results to the new account card • Designated Supervisor(s) approving the new account shall only approve an account if an OFAC search is attached to the new account card. If a positive identification is made, the AML Compliance Officer or designee shall be notified immediately. AML Officer or designee: If a positive identification is found, 1. Block accounts subject to sanctions 2. Cancel open orders for blocked accounts 3. Notify the OSJ Branch Manager and the account's RR, when an account or security is blocked 4. Notify OFAC by FAX within 10 days of blocking an account 5. Notify Dreyfus Service Corporation with respect to funds in a blocked account having been swept into the Dreyfus Money Market account. AML Officer or designee: • Review, initial (or sign), date and retain the OFAC screening report • Maintain log of blocked accounts
Record	• Record of each new account accompanied by the OFAC search results • OFAC screening report results, subsequent OFAC searches undertaken, if any, and any actions taken • Notifications to OFAC

The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) is responsible for publishing sanctions against persons, corporations, and other entities including foreign governments that have been identified by the U.S. Government as engaging in criminal activities including drug trafficking and terrorist activities. OFAC requirements apply to all persons and entities under U.S. jurisdiction, including foreign branches of U.S. institutions. This also includes foreign institutions that operate in the U.S. Alpine is obligated to check its accounts against the lists of blockings to ensure it does not engage in prohibited transactions which include securities transactions and transfer of assets out of a blocked account or to a blocked person or entity. Alpine has procedures to monitor the OFAC lists and comply with requirements to block property and notify OFAC when required. Questions regarding Alpine's program should be referred to the AML Officer or designee. More information is also available at the OFAC web site at *www.treas.gov/ofac*.

Before opening an account, and on an ongoing basis, the parties enumerated above will check to ensure that a customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC prior to approving or opening an account.

Because the SDN list and listings of economic sanctions and embargoes are updated frequently, Alpine will consult them on a regular basis and subscribe to receive any available updates when they occur. With respect to the SDN list, Alpine may also access that list through various software programs to ensure speed and accuracy. *See also*FINRA's OFAC Search Tool that screens names against the SDN list.

If Alpine determines that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC within 10 days. Alpine will also call the OFAC Hotline at (800) 540-6322 immediately.

The property of sanctioned persons or entities will be blocked and transfer of assets prevented for persons or entities included on the OFAC list of blocked persons or entities. In addition, Alpine will block securities issued

by sanctioned countries and other sanctioned issuers. Information about sanctions is divided into several categories including:

- Persons and entities subject to sanctions, *Special Designated Nationals and Blocked Persons* (SDN list)
- Persons and entities engaged in drug trafficking, *Specially Designated Narcotics Traffickers* (SDNTKs)
- Terrorists and terrorist organizations, *Specially Designated Terrorists* (SDTs)
- Countries, governments, and other entities subject to sanctions

The term "OFAC list" in this section includes all sanctions published by OFAC even though the information may appear in multiple lists.

9.6.1 Prohibited Transactions

Alpine is prohibited from conducting transactions in any account on behalf of a sanctioned party or in certain blocked securities. Securities and funds may not be released and securities transactions may not be executed. Securities and funds may be deposited to a blocked account, but no securities or funds will be released until the account is no longer subject to sanctions. Funds or securities may not be transferred to sanctioned parties.

Because transactions are prohibited, all open orders for a blocked account will be cancelled.

9.6.2 Blocking Requirements

Blocking requirements are generally triggered under the following circumstances:

- An account is opened for someone included on an OFAC list.
- The owner of an existing account is added to an OFAC list.
- A security is identified in a customer account where the issuer is the subject of sanctions.
- A request is made by a customer to pay or transfer funds or securities to a blocked person or entity.

While title to blocked property remains with the blocked person or entity, transactions affecting the property (including transfer of the assets) cannot be made without authorization from OFAC. Debits to blocked accounts are prohibited, but credits may be accepted. Cash balances in blocked accounts must earn interest at commercially reasonable rates. Blocked securities may not be paid, withdrawn, transferred (even in book transfer), endorsed, guaranteed, or otherwise dealt in.

It is not a violation to open an account for a blocked person. The violation occurs when the account is not frozen and assets are allowed to transfer out of the account. In addition, OFAC restrictions may vary depending on the blocked person or entity; details of blocking requirements are explained on the OFAC web site.

9.6.3 Monitoring Procedures

Monitoring is to be conducted as follows:

- Operations personnel and Supervisors approving new accounts are provided with a list of the countries included on the OFAC countries list, to watch for new accounts to be opened for or requests to transfer funds or securities to residents of those countries. The AML Officer or designee shall provide an updated list each month by email to all operations personnel and supervisors.
- Alpine's retail sales staff undertakes an OFAC search utilizing the www.treas.gov/ofac web site for each new account and attaches the OFAC search results to the new account form.
- Alpine's AML Officer or designee performs a daily review of the OFAC screenings report provided by CSS Hosted Solutions, LLC. The OFAC screening report identifies potential matches to the OFAC SDN List or Specially Designated Nationals Alias List for new or changed accounts. In addition, the AML Officer or designee performs a bi-weekly review of the following reports for trade and/or transmittal activities involving accounts that reside in a non-cooperative countries and/or blocked countries:
  - Account Activity in Non-Cooperative and Blocked Countries Report
  - Account in Non-Cooperative Countries Report

- Foreign Account Activity Report:

To evidence review, a report is produced that is reviewed, initialed (or signed) and retained by the AML Officer or designee.

9.6.3.1 Other Requests To Monitor Accounts

Regulators or law enforcement agencies may ask the industry's cooperation in identifying accounts for individuals or entities under investigation or suspected of criminal activities.

The AML Officer or designee is responsible for responding to such requests; providing the necessary information; and retaining records of requests, reviews conducted pursuant to requests, and information provided to authorities.

9.6.4 Blocking Property And Disbursements

Any blocked account will not be permitted to engage in transactions other than the acceptance of deposits of funds or securities. Open orders of blocked accounts will be cancelled.

Disbursements of funds or securities may not be made to sanctioned parties. The AML Officer or designee will instruct Alpine's Operations Department to withhold requests for disbursements from blocked accounts and will maintain a log of all accounts that have been blocked.

9.6.4.1 Reporting Blocked Property And Legal Actions

When an account or disbursement is blocked or a blocked security is identified, OFAC will be notified within 10 days of blocking. If Alpine blocks an account or security, the AML Officer or designee will file the necessary report with OFAC. The AML Officer or designee will be responsible to retain copies of reports filed by Alpine in a file of blocked accounts or securities. Information to be reported includes:

- Owner or account party
- Property and property location
- Account number
- Actual or estimated value
- Date property was blocked
- Copy of the payment or transfer instructions
- Confirmation that funds have been deposited in a blocked account that is identified as blocked
- Name and phone number of Alpine's AML Officer

For rejected disbursements, the following information is to be filed:

- Name and address of the transferee financial institution
- Date and amount of the transfer
- Copy of the payment or transfer instructions
- Basis for rejection
- Name and phone number of Alpine's AML Officer

U.S. persons involved in litigation, arbitration, or other binding alternative dispute resolution proceedings regarding blocked property must provide notice to OFAC. Copies of all documents associated with the proceedings will be submitted by the AML Officer or designee to the OFAC Chief Counsel at the U.S. Treasury Department within 10 days of their filing. In addition, information about the scheduling of any hearing or status conference will be faxed to OFAC's Chief Counsel.

9.6.4.2 Annual Report Of Blocked Property

On an annual basis by September 30th, the AML Officer or designee shall file Form TDF 90-22.50 with OFAC for any blocked property held as of June 30.

9.6.5 Penalties for Non-Compliance with OFAC Rules and Regulations

Depending on the program, criminal penalties for willful violations can include fines ranging up to $20 million and imprisonment of up to 30 years, and up to $1,075,000 in civil penalties for each violation.

9.7 Customer Identification Program (CIP)

Rules/Resources:USA PATRIOT Act Section 326; Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart B; FINRA Notice to Members 03-34; FinCEN Frequently Asked Questions: http://www.fincen.gov/cip_faq.html; FinCEN No-Action position on CIP requirements under clearing arrangements: FIN-2008-G002; Guidance on Obtaining and Retaining Beneficial Ownership Information, FinCEN Guidance, FIN-2010-G001 March 5, 2010

In addition to the information Alpine must collect under FINRA Rule 2010 (Standards of Commercial Honor and Principles of Trade), FINRA Rule 2111 (Recommendations to Customers - Suitability), NASD 3110 (Books and Records) and Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3(a)(9) (Beneficial Ownership regarding Cash and Margin Accounts) and 17a-3(a)(17) (Customer Accounts), Alpine has established, documented and maintained a written Customer Identification Program (CIP). Alpine will collect certain minimum customer identification information from each customer who opens an account; utilize risk-based measures to verify the identity of each customer who opens an account; record customer identification information and the verification methods and results; provide the required adequate CIP notice to customers that Alpine will seek identification information to verify their identities; and compare customer identification information with government-provided lists of suspected terrorists, once such lists have been issued by the government.

Requirements for employees opening accounts as explained in the chapter *ACCOUNTS* are duplicated in this section to consolidate all AML requirements within this chapter.

9.7.1 Required Customer Information

Prior to opening an account, Alpine will collect the following information for all accounts, if applicable, for any person, entity or organization that is opening a new account and whose name is on the account, absent some exceptions:

- **Name**
- **Date of birth,** for an individual
- **Address:**
  - for an individual, residential or business street address. If no street address exists or is available, an APO or FPO box number or the residential or business street address of a next of kin or another contact individual
  - for a non-individual (corporation, trust, *etc.*) a principal place of business, local office, or other physical location.
- **Taxpayer identification number** for a U.S. person (U.S. citizen or non-individual established or organized under U.S. or state laws).
- **Identification number for non-U.S. person** which may include a taxpayer ID number; passport number and country of issuance; alien identification card number; or the number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photo or similar safeguard.

In the case of a customer who has applied for a taxpayer identification number but has not yet received it, notation must be made on the new account application that the taxpayer ID has been applied for. The account will be restricted to liquidating transactions if the taxpayer ID number is not received within 30 days of opening the account.

Alpine may rely on another financial institutional to obtain this information, prior to opening an account. Please refer to the section titled "Reliance on Another Financial Institution for Identity Verification". The use of the term "customer" in this section is also intended to include prospective customers.

9.7.1.1 Customer Identity Verification

This section is duplicated from Chapter 11.

Responsibility	• OSJ Branch Manager, President or their designees ("Designated Supervisor(s)")
Resources	• New account application and other customer ID information
Frequency	• When accounts are opened
Action	• Before the Designated Supervisor approves an account, determine that customer identification (ID) verification information is included with the new account application and that it meets Alpine's requirements • For non-documentary verification, check the information included with the new account application for completeness and consistency with other customer-provided information (name, address, phone number, taxpayer ID number, *etc.*) • For unacceptable verification information (incomplete, inconsistent), return the application to the RR for further information or disapprove the account
Record	• Each Customer file shall contain the New Account Application and records that include customer ID verification as well as the Designated Supervisor's signature signifying approval

When opening new accounts, the customer's identity must be verified, as required by federal law. Customer identification (ID) information must be completed on the new account application.

9.7.1.2 Exclusions from the CIP Rule

Customer ID verification does NOT apply to accounts for:

- persons with an existing account at Alpine (unless the account requires approval by the AML Officer or designee)
- banks
- governmental entities
- issuers of listed equity securities
- other financial institutions subject to regulation by the SEC, CFTC, Federal Reserve Board, OCC, FDIC, Office of Thrift Supervision, or the National Credit Union Administration
- persons opening accounts to participate in an ERISA plan
- Intermediaries not identified as the accountholder (such as underlying beneficial owners or sub-account holders. See the section titled "Omnibus and Sub-Accounts" for more information.

9.7.1.3 Customers Who Refuse to Provide Information

If a potential or existing customer either refuses to provide the information described above when requested or appears to have intentionally provided misleading information, Alpine will not open a new account and, after considering the risks involved, may consider closing any existing account. In either case, our AML Officer or

designee should be notified so that we can determine whether we should report the situation to FinCEN on a SAR-SF.

9.7.1.4 Accounts Requiring Approval By The AML Officer or Designee

The following accounts require review and approval by the AML Officer or designee at the time of opening. The AML Officer or designee may require additional customer identification information for these accounts.

- **Numbered accounts** (accounts designating a number rather than a name as the account name).
- **Any account requesting confidential handling** of its name, mailing of confirmation and statements, *etc.*
- **Accounts domiciled in high risk countries.** Accounts domiciled in countries identified by OFAC or the Financial Action Task Force on Money Laundering (FATF) as having inadequate anti-money laundering standards or representing high risk for crime and corruption.
- **Foreign public officials.** Includes individuals in high offices of foreign governments, political party officials and their families and close associates (if known and/or readily identifiable).
- **Correspondent and Private Banking accounts.** See the section *Due Diligence For Correspondent And Private Banking Accounts.*

If the accounts noted above are introduced by a correspondent firm, Alpine may rely on another financial institution to perform the customer identification program requirements. Please refer to the section titled "Reliance on Another Financial Institution for Identity Verification".

9.7.1.5 Omnibus And Sub-Accounts

Rules/Resources: SEC Q and A Regarding the Broker-Dealer Customer Identification Program Rule, October 1, 2003

Omnibus and sub-accounts are sometimes established by or on behalf of financial intermediaries for the purpose of executing transactions that will clear or settle at another financial institution or for delivering assets to the custody account of the beneficial owner at another financial institution. Limited information about the beneficial owner is used primarily to assist the financial intermediary with recordkeeping or to establish sub-accounts to hold positions to be transferred to another financial institution. Transactions are initiated by the financial intermediary and the beneficial owner has no direct control over the omnibus or sub-accounts.

Under these circumstances, Alpine is not required to look through the intermediary to the underlying beneficial owners, if the intermediary is identified as the accountholder. In the event the intermediary identified as the account holder's identity cannot be adequately verified using documentary and non-documentary methods, identity information on the persons or entities controlling the account will be required.

9.7.1.6 Third Party Accounts

Please refer to Chapter 11 of Alpine's written supervisory procedures for information on the documentation requirements for third party accounts in the section titled "Third Party Accounts".

9.7.1.7 Accounts For Non-Individuals

Account documents usually obtained for non-individual accounts (trust instruments, corporate authorization, partnership agreements, government-issued business license, *etc.*) will usually satisfy customer ID requirements. In the case of corporations, a corporate authorization is required. These documents must be obtained within 30 days of account opening to satisfy the requirement.

9.7.2 Verifying Information

Based on the risk, and to the extent reasonable and practicable, Alpine will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information Alpine receives about our customers. The OSJ Branch Manager or designee will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies). With respect to customers introduced by correspondent firm, Alpine will reasonably rely on the performance of the financial institution with respect to customer verification. Please refer to the section titled "Reliance on Another Financial Institution for Identity Verification" for more information.

Alpine will verify customer identity through documentary means, non-documentary means or both as enumerated below. Alpine will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. Alpine may also use non-documentary means, if Alpine is still uncertain about whether we know the true identity of the customer. In verifying the information, Alpine will consider whether the identifying information that we receive, such as the customer's name, street address, zip code, telephone number (if provided), date of birth and Social Security number, allow us to determine that we have a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

Appropriate documents for verifying the identity of customers include the following:

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument.

Alpine understands that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.

Alpine will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, Alpine may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, Alpine may, pending verification, restrict the types of transactions or dollar amount of transactions. If Alpine find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, Alpine will, after internal consultation with the firm's AML Officer or designee, file a SAR-SF in accordance with applicable laws and regulations.

9.7.2.1 Non-Documentary Methods Of Verifying Customer Identification

Alpine will use non-documentary methods of verification when:

- (1) the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;
- (2) the firm is unfamiliar with the documents the customer presents for identification verification;
- (3) the customer and firm do not have face-to-face contact; and
- (4) there are other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.
- (5) Other circumstances, at the discretion of the RR's supervisor, New Accounts, and/or the AML Officer or designee, where Alpine is unable to verify the customer's identity.

In these circumstances, a non-documentary method must be indicated by the RR on the new account application:

- Direct customer contact information
- Information from a consumer reporting agency or other database
- References from another financial institution
- A financial statement from a bank
- Copy of a utility bill

9.7.2.2 Additional Verification For Certain Customers

Alpine recognizes that the risk that we may not know the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by the U.S. as a primary money laundering jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory. Alpine will identify customers that pose a heightened risk of not being properly identified. Alpine will also take the following additional measures that may be used to obtain information about the identity of the individuals associated with the customer when standard documentary methods prove to be insufficient.

For the following types of customers, a minimum of TWO forms of customer ID are required in addition to review and approval by the AML Officer or designee **prior to** opening the account:

- Numbered accounts
- Accounts domiciled in high-risk countries included on the Treasury Dept. OFAC list (check with Operations personnel for a list of those countries or go to http://www.ustreas.gov/offices/eotffc/ofac/sanctions/index.html)
- Accounts for foreign public officials (individuals in high office in other countries, their families and close associates, political party officials)

9.7.2.3 Lack Of Customer ID Verification

When Alpine cannot form a reasonable belief that we know the true identity of a customer, Alpine will:

1. not open an account;
2. impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity;
3. close an account after attempts to verify customer's identity fail; and
4. determine whether it is necessary to file a SAR-SF in accordance with applicable laws and regulations.

Questions regarding accounts that do not comply with requirements to verify customer ID should be referred to the AML Officer or designee.

9.7.3 Recordkeeping

Alpine will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. Alpine will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, Alpine will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. Alpine will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. Alpine will retain records of all identification information for five years after the account has been closed and will retain records made about verification of the customer's identity for five years after the record is made.

9.7.4 Comparison with Government-Provided Lists of Terrorists

At such time as Alpine receives notice that a federal government agency has issued a list of known or suspected terrorists and identified the list as a list for CIP purposes, Alpine will, within a reasonable period of time after an account is opened (or earlier, if required by another federal law or regulation or federal directive issued in connection with an applicable list), determine whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any federal government agency and designated as such by Treasury in consultation with the federal functional regulators. Alpine will follow all federal directives issued in connection with such lists.

Alpine will continue to comply separately with OFAC rules prohibiting transactions with certain foreign countries or their nationals.

9.7.5 Notice to Customers

Rules/Resources: 31 C.F.R. □103.122(b)(5)

Alpine will provide notice to customers that Alpine is requesting information from them to verify their identities, as required by federal law. Customers are provided notice, prior to opening an account, that their identification will be verified. This notice may be on Alpine's web site, on new account applications, or in other disclosures provided at the time of account opening and may include, but not be limited to, the following:

Important Information about Procedures for Opening This Account

To help the government fight the funding of terrorism and money laundering activities, federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account. Client is required to provide the following information, among other items, on new account forms; name, address, date of birth and other information that will allow Alpine to confirm Client's identity. In addition, your broker may ask to see a valid driver's license or other identifying documents.

9.7.6 Reliance on Another Financial Institution for Identity Verification

Rules/Resources: 31 C.F.R. § 103.122(b)(6), No-Action Letters to the Securities Industry and Financial Markets Association (SIFMA) (formerly known as the Securities Industry Association (SIA)) (February 12, 2004; February 10, 2005; July 11, 2006; and January 10, 2008). (The letters provide staff guidance regarding the extent to which a broker-dealer may rely on an investment adviser to conduct the required elements of the CIP rule, prior to such adviser being subject to an AML rule.)

In its clearing functions, Alpine will, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of our CIP with respect to any customer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings or other financial transactions:

- when such reliance is reasonable under the circumstances;
- when the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements of 31 U.S.C. § 5318(h), and is regulated by a federal functional regulator; and
- when Alpine has entered into a contract with the other financial institution to perform these functions and requiring it to certify annually to us that it has implemented its anti-money laundering program and that it will perform (or its agent will perform) specified requirements of the customer identification program.

9.7.6.1 Reliance on Registered Investor Adviser Accounts

Rules/Resources:SEC Division of Market Regulation No-Action Letter to SIFMA dated January 11, 2011: http://www.sec.gov/divisions/marketreg/mr-noaction/2011/sifma011111.pdf

For accounts established by registered investment advisers, Alpine may rely on the adviser to have obtained information to comply with federal Customer Identification Program (CIP) rules under the following circumstances:

- it is reasonable to rely on the adviser's assurances;
- the adviser is federally regulated (state-only registered IAs do not qualify); and
- the adviser signs an agreement that it will annually certify to Alpine that it has implemented an anti-money laundering program and will perform (or its agents will perform) specified requirements of Alpine's CIP.

9.8 Due Diligence For Correspondent And Private Banking Accounts

Rules/Resources: Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart F; USA PATRIOT Act Section 312 and 313; FinCEN Fact Sheet (http://www.fincen.gov/312factsheet.pdf)

9.8.1 Definitions

Correspondent account: Includes any account established for a foreign financial institution to receive deposits from, or to make payments or other disbursements on behalf of, the foreign institution, or to handle other financial transactions related to such foreign financial institution. This type of account presumes a formal relationship through which the financial institution provides regular services.

For broker-dealers, correspondent accounts established on behalf of foreign financial institutions include, but are not limited to: (1) accounts to purchase, sell, lend, or otherwise hold securities, including securities repurchase programs; (2) prime brokerage accounts that clear and settle securities transactions for clients; (3) accounts for trading foreign currency; (4) custody accounts for holding securities or other assets in connection with securities transactions as collateral; and (5) over-the-counter derivative contracts.

Account: Any formal relationship established with a broker or dealer in securities to provide regular services to effect transactions in securities, including but not limited to, the purchase or sale of securities and securities loaned and borrowed activity, and to hold securities or other assets for safekeeping or as collateral.

Foreign bank: defined under the Bank Secrecy Act as a bank organized under foreign law, or an agency, branch, or bank office located outside the United States. The term does not include an agent, agency, branch or office within the U.S. of a bank organized under foreign law.

Foreign financial institution: defined as:

(1) a foreign bank;

(2) any branch or office located outside the United States of a broker-dealer; futures commission merchant or introducing broker; or open-end mutual fund company;

(3) any other person organized under foreign law (other than a branch or office of such person in the United States) that, if it were located in the United States, would be a broker-dealer; futures commission merchant or introducing broker; or open-end mutual fund company; and

(4) any person organized under foreign law (other than a branch or office of such person in the United States) that is engaged in the business of, and is readily identifiable as: (a) a currency dealer or exchanger; or (b) a money transmitter.

A person, however, is not "engaged in the business" of a currency dealer, a currency exchanger or a money transmitter if such transactions are merely incidental to the person's business.

Foreign shell bank: a foreign bank without a physical presence in any country.

Regulated affiliate: a foreign shell bank that (1) is an affiliate of a depository institution, credit union, or foreign bank that maintains a physical presence in the United States or a foreign country, as applicable; and (2) is subject to supervision by a banking authority in the foreign country regulating such affiliated depository institution, credit union, or foreign bank.

Responsibility	• AML Officer or designee
Resources	• New account application • Foreign bank certification • Information about a foreign bank subsequent to opening that indicates it is a foreign shell bank where an account may not be maintained
Frequency	• As required when accounts are opened • Monthly - review of accounts identified for due diligence reviews
Action	• Conduct due diligence for correspondent and private banking accounts • For foreign bank accounts: o Review certification to determine: ▪ All required information is included ▪ Inconsistencies (*i.e.*, location of the foreign bank's regulated affiliate is consistent with the designated banking authority that supervises the foreign bank and its regulated affiliate) o Ensure procedures are in place to restrict transactions in accounts that do not provide certification within 30 days of opening the account o Close existing prohibited accounts for foreign shell banks o Review re-certifications o Ensure procedures are in place to re-certify foreign banks within three years of original certification
Record	• Record of the AML Officer's or designee's review is maintained in new account records on the applicable form: o New account application o Certification form o Re-certification form • Records of closing or restricting accounts are retained with new account records

9.8.2 Due Diligence and Enhanced Due Diligence Requirements For Correspondent Accounts of Foreign Financial Institutions

Rules/Resources: 31 C.F.R. §§ 103.175, 103.176, FIN-2006-G009 Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industries (May 10, 2006).

Alpine will conduct an inquiry to determine whether a foreign financial institution has a correspondent account established, maintained, administered or managed by the firm.

If Alpine has correspondent accounts for foreign financial institutions, Alpine will assess the money laundering risk posed, based on a consideration of relevant risk factors. Alpine can apply all or a subset of these risk factors depending on the nature of the foreign financial institutions and the relative money laundering risk posed by such institutions.

The U.S. Department of Treasury has established the following minimum due diligence requirements:

- determine whether the account is subject to enhanced due diligence
- assess the money laundering risk posed, based on risk factors
- apply risk-based policies, procedures and controls to each account, including periodic review of activity

The relevant risk factors can include:

- The nature of the foreign financial institution's business and the markets it serves; the type, purpose and anticipated activity of such correspondent account;
- the nature and duration of the firm's relationship with the foreign financial institution and its affiliates;
- the anti-money laundering and supervisory regime of the jurisdiction that issued the foreign financial institution's charter or license and, to the extent reasonably available, the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered; and
- any information known or reasonably available to the covered financial institution about the foreign financial institution's anti-money laundering record.

Alpine will apply our risk-based due diligence procedures and controls to each financial foreign institution correspondent account on an ongoing basis. This includes periodically reviewing the activity of each foreign financial institution correspondent sufficient to ensure whether the nature and volume of account activity is generally consistent with the information regarding the purpose and expected account activity and to ensure that the firm can adequately identify suspicious transactions. Ordinarily, Alpine will not conduct this periodic review by scrutinizing every transaction taking place within the account. One procedure Alpine may use instead is to use any account profiles for our correspondent accounts (if we maintain these) that we ordinarily use to anticipate how the account might be used and the expected volume of activity to help establish baselines for detecting unusual activity.

Correspondent accounts for foreign financial institutions are forwarded to the AML Officer or designee, at the time of opening, for review.

- Review the account's home country vs. OFAC lists of jurisdictions of money laundering concern and blocked persons.
    - If identified on an OFAC list, report the account and close it.
- Review new account information about the account including source of revenue and assets, whether the person/entity has existing accounts with Alpine, length of time the RR has known the account, who referred the account, and other available information about account background and how the account came to Alpine.
- If there is inadequate information or due diligence procedures cannot be performed, refuse to open the account or close an existing account.

    - File a SAR, if appropriate.

- If the account is approved for opening, determine whether ongoing review is necessary.

    - If ongoing review is appropriate, establish duplicate statements or another method for review of account activity by the AML Officer.
    - Review will include identifying patterns of securities transactions and securities/money transfers that may be indicative of money laundering activity, and report such activity if necessary and close the account.

9.8.2.1 Correspondent Accounts Introduced by a Correspondent Firm (or Introducing Firm)

In those cases where Alpine has a formal relationship with any final institution with which it has executed a clearing or carrying agreement, Alpine understands its obligation to perform due diligence pursuant to the correspondent rule with respect to its carrying agreement with a foreign financial institution. However, Alpine will not have a formal relationship and thus will not have an account subject to the due diligence provisions of the

correspondent account rule, with a foreign financial institution introduced to us under a clearing agreement unless Alpine engages in activities that obligate us to make a suitability determination with respect to securities transactions conducted through the introduced foreign financial institution accounts.

In these cases, Alpine will consider the money laundering risks posed by the introducing firm, including any information Alpine acquires about the account base of the introducing firm's ordinary course of business and through the application of the introducing firm's anti-money laundering policies, procedures and controls.

9.8.2.2 Enhanced Due Diligence For Foreign Banks

Rules/Resources: 31 C.F.R. §§ 103.175, 103.176.

Alpine will assess (and perform enhanced due diligence) any correspondent accounts for foreign financial institutions to determine whether they are correspondent accounts that have been established, maintained, administered or managed for any foreign bank that operates under:

(1) an offshore banking license;

(2) a banking license issued by a foreign country that has been designated as non-cooperative with international anti-money laundering principles or procedures by an intergovernmental group or organization of which the United States is a member and with which designation the U.S. representative to the group or organization concurs; or

(3) a banking license issued by a foreign country that has been designated by the Secretary of the Treasury as warranting special measures due to money laundering concerns.

If Alpine determines that it has any correspondent accounts for these specified foreign banks, Alpine will perform enhanced due diligence on these correspondent accounts. The enhanced due diligence that we will perform for each correspondent account will include, at a minimum, procedures to take reasonable steps to:

(1) conduct enhanced scrutiny of the correspondent account to guard against money laundering and to identify and report any suspicious transactions. Such scrutiny will not only reflect the risk assessment that is described in Section 8.a. above, but will also include procedures to, as appropriate:

(i) obtain (e.g., using a questionnaire) and consider information related to the foreign bank's AML program to assess the extent to which the foreign bank's correspondent account may expose us to any risk of money laundering;

(ii) monitor transactions to, from or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity (this monitoring may be conducted manually or electronically and may be done on an individual account basis or by product activity); and

(iii) obtain information from the foreign bank about the identity of any person with authority to direct transactions through any correspondent account that is a payable-through account (a correspondent account maintained for a foreign bank through which the foreign bank permits its customer to engage, either directly or through a subaccount, in banking activities) and the sources and beneficial owners of funds or other assets in the payable-through account.

(2) determine whether the foreign bank maintains correspondent accounts for other foreign banks that enable those other foreign banks to gain access to the correspondent account under review and, if so, to take reasonable steps to obtain information to assess and mitigate the money laundering risks associated with such accounts, including, as appropriate, the identity of those other foreign banks; and

(3) if the foreign bank's shares are not publicly traded, determine the identity of each owner and the nature and extent of each owner's ownership interest. We understand that for purposes of determining a private foreign bank's ownership, an "owner" is any person who directly or indirectly owns, controls or has the power to vote 10

percent or more of any class of securities of a foreign bank. Alpine also understands that members of the same family shall be considered to be one person.

Refer the account to the AML Officer or designee to:

- conduct appropriate enhanced scrutiny;
- determine whether the foreign bank itself offers correspondent accounts to other foreign banks (*i.e.*, nested accounts) and, as appropriate, identify such foreign bank customers and conduct additional due diligence on them; and
- identify the owners of such foreign bank, if its shares are not publicly traded.
- determine whether the account appears on any OFAC list;
- approve or reject the account.
- determine whether ongoing review is necessary.
    - If yes, establish duplicate statements or other method for ongoing review.

- report the account, if appropriate.

9.8.2.3 Special Procedures When Due Diligence or Enhanced Due Diligence Cannot Be Performed

Rules/Resources: 31 C.F.R. §§ 103.175, 103.176.

In the event there are circumstances in which Alpine cannot perform appropriate due diligence with respect to a correspondent account, the AML Officer or designee will determine, at a minimum, whether to refuse to open the account, suspend transaction activity, file a SAR-SF, close the correspondent account and/or take other appropriate action.

9.8.2.4 Prohibition Against Correspondent Accounts For Foreign Shell Banks

Rules/Resources: Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart F; USA PATRIOT Act Section 313

Alpine is prohibited from establishing, maintaining, administering, or managing a correspondent account in the United States for an unregulated foreign shell bank. The prohibition does not apply to a foreign shell bank that is a regulated affiliate. If an account is inadvertently opened for an unregulated foreign shell bank, the AML Officer or designee must be notified and the account will be immediately closed.

9.8.3 Foreign Bank Certification

Rules/Resources: FinCEN Frequently Asked Questions re Certification: http://www.fincen.gov/faqsguidance.pdf, Rules: 31 C.F.R. §§ 103.175, 103.177, 31 C.F.R., Pt. 103, Subpt. I, App. A (Certification Regarding Correspondent Accounts for Foreign Banks); FIN-2006-G003: Frequently Asked Questions: Foreign Bank Recertifications under 31 C.F.R. § 103.77 (February 3, 2006).

When opening an account for a foreign bank, Alpine is obligated to ensure the bank is not an unregulated foreign shell bank and must obtain information about the foreign bank's owners and an agent for service of process. Alpine will require our foreign bank account holders to identify the owners of the foreign bank if it is not publicly traded, the name and street address of a person who resides in the United States and is authorized and has agreed to act as agent for acceptance of legal process, and an assurance that the foreign bank is not a shell bank nor is it facilitating activity of a shell bank. In lieu of this information the foreign bank may submit the Certification Regarding Correspondent Accounts For Foreign Banks provided in the BSA regulations to the AML Officer or designee. Alpine will re-certify when we believe that the information is no longer accurate or at least once every three years.

9.8.4 Recordkeeping for Correspondent Accounts for Foreign Banks

Rules/Resources: 31 C.F.R. §§ 103.175, 103.177.

Alpine will keep records identifying the owners of foreign banks with U.S. correspondent accounts and the name and address of the U.S. agent for service of legal process for those banks.

9.8.5 Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationships with Foreign Bank

Rules/Resources: USA PATRIOT Act Section 313

Upon receipt of a written request from a federal law enforcement officer for information identifying the non-publicly traded owners of any foreign bank for which we maintain a correspondent account for a foreign bank in the United States and/or the name and address of a person residing in the United States who is an agent to accept service of legal process for a foreign bank's correspondent account, the AML Officer or designee will provide that information to the requesting officer not later than 7 days after receipt of the request.

The AML Officer or designee will close, within 10 days, any correspondent account for a foreign bank that we learn from FinCEN or the Department of Justice has failed to comply with a summons or subpoena issued by the Secretary of the Treasury or the Attorney General of the United States or has failed to contest such a summons or subpoena. We will scrutinize any foreign bank's correspondent account activity during that 10-day period to ensure that any suspicious activity is appropriately reported and to ensure that no new positions are established in these foreign bank's correspondent accounts.

9.9 Due Diligence For Private Banking Accounts

Rules/Resources: Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart F

9.9.1 Definitions

Private banking account: A private banking account is an account that is established or maintained for the benefit of one or more non-U.S. persons, requires minimum aggregate deposit of funds or other assets of not less than $1,000,000, and is assigned to a bank employee who is a liaison between the financial institution and the non-U.S. person. If the account otherwise satisfies the definition but the institution does **not** require a minimum balance of $1,000,000, the account does not qualify as a private banking account.

Senior foreign political figure includes:

- a current or former senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government, whether or not they are or were elected officials
- a senior official of a major foreign political party
- a senior executive of a foreign government-owned commercial enterprise (Senior executives are individuals with substantial authority over policy, operations, or the use of government-owned resources.)
- immediate family members of the above, and those who are widely and publicly known (or actually known) close associates of a senior foreign political figure
- a corporation, business, or other entity formed by or for the benefit of one of the above individuals
- a person "widely and publicly known" as a close associate of such a person

Proceeds of foreign corruption: any asset acquired by, through, or on behalf of a senior foreign political figure through misappropriation, theft, or embezzlement of public funds, the unlawful conversion of property of a foreign government, or through acts of bribery or extortion, and include any other property into which any such assets have been transformed or converted.

Alpine will review our accounts to determine whether we offer any private banking accounts and we will conduct due diligence on such accounts. This due diligence will include, at least, (1) ascertaining the identity of all nominal holders and holders of any beneficial ownership interest in the account (including information on those holders' lines of business and sources of wealth); (2) ascertaining the source of funds deposited into the account; (3) ascertaining whether any such holder may be a senior foreign political figure; and (4) detecting and reporting, in accordance with applicable laws and regulations, any known or suspected money laundering, or use of the proceeds of foreign corruption.

Alpine will review public information, including information available in Internet databases, to determine whether any private banking account holders are senior foreign political figures. If we discover information indicating that a particular private banking account holder may be a senior foreign political figure, and upon taking additional reasonable steps to confirm this information, we determine that the individual is, in fact, a senior foreign political figure, we will conduct additional enhanced due diligence to detect and report transactions that may involve money laundering or the proceeds of foreign corruption.

In so doing, Alpine will consider the risks that the funds in the account may be the proceeds of foreign corruption by determining the purpose and use of the private banking account, location of the account holder(s), source of funds in the account, type of transactions conducted through the account and jurisdictions involved in such transactions. The degree of scrutiny we will apply will depend on various risk factors, including, but not limited to, whether the jurisdiction the senior foreign political figure is from is one in which current or former political figures have been implicated in corruption and the length of time that a former political figure was in office. Our enhanced due diligence might include, depending on the risk factors, probing the account holder's employment history, scrutinizing the account holder's source(s) of funds, and monitoring transactions to the extent necessary to detect and report proceeds of foreign corruption, and reviewing monies coming from government, government controlled or government enterprise accounts (beyond salary amounts).

If Alpine does not find information indicating that a private banking account holder is a senior foreign political figure, and the account holder states that he or she is not a senior foreign political figure, then Alpine may make an assessment if a higher risk for money laundering, nevertheless, exists independent of the classification. If a higher risk is apparent, we will consider additional due diligence measures.

In either case, if due diligence (or the required enhanced due diligence, if the account holder is a senior foreign political figure) cannot be performed adequately, Alpine will, after consultation with the firm's AML Officer or designee and, as appropriate, not open the account, suspend the transaction activity, file a SAR-SF or close the account.

9.9.2 Enhanced Scrutiny For Accounts Of Senior Foreign Political Figures

Accounts for senior foreign political figures (including persons and entities defined in this section) are subject to enhanced scrutiny. Prior to opening, the account is referred to the AML Officer or designee for review and approval and may consider the following steps:

- Review the account's home country vs. OFAC lists of jurisdictions of money laundering concern and blocked persons.
    - If identified on an OFAC list, report the account and close it.
- Review new account information about the account including employment history, sources of income and assets, whether the person/entity has existing accounts with Alpine, length of time the RR has known the account, who referred the account, and other available information about account background of the account and how the account came to Alpine.
- If there is inadequate information or due diligence procedures cannot be performed, refuse to open the account or close an existing account.

    - File a SAR, if appropriate.

- If the account is approved for opening, determine whether ongoing review is necessary.

- If ongoing review is appropriate, establish duplicate statements or another method for review of account activity by the AML Officer or designee.
- Review will include identifying patterns of securities transactions and securities/money transfers that may be indicative of money laundering activity, and report such activity if necessary and close the account.

9.9.3 Private Banking Accounts Introduced by a Correspondent Firm (or Introducing Firm)

In those cases where Alpine does not impose aggregate minimum account requirements of not less than $1,000,000 on an introduced account for a non-U.S. person and does not assign an officer, employee, or agent to act as a liaison between the clearing firm and such an account, the introduced account will not be considered a private banking account of the clearing firm.

In these cases, Alpine will consider the money laundering risks posed by the introducing firm, including any information Alpine firm acquires about the account base of the introducing firm's ordinary course of business and through the application of the introducing firm's anti-money laundering policies , procedures and controls.

9.10 Compliance with FinCEN's Issuance of Special Measures Against Foreign Jurisdictions, Financial Institutions or International Transactions of Primary Money Laundering Concern

Rules/Resources: USA PATRIOT Act Section 311; Bank Secrecy Act 31 CFR Chapter X Part 1010 Subpart F; FINRA Notice to Members 06-41; FinCEN information on all special measures issued: http://www.fincen.gov/reg_section311.html

Responsibility	• AML Officer or designee
Resources	• FinCEN notification of special measures against named entities • Transaction records • Customer account records
Frequency	• As required when notified by FinCEN
Action	• Establish blocks on opening accounts for named entities • Notify correspondent accountholders • Review transactions to identify indirect use of correspondent accounts and close such accounts
Record	• Notices from FinCEN • Notification to correspondent accountholders • Transactions reviewed, identification of indirect use, and action taken

If FinCEN issues a final rule imposing a special measure against one or more foreign jurisdictions or financial institutions, classes of international transactions or types of accounts deeming them to be of primary money laundering concern, Alpine understands that we must read FinCEN's final rule and follow any prescriptions or prohibitions contained in that rule. For example, if the final rule deems a certain bank and its subsidiaries (Specified Bank) to be of primary money laundering concerns, a special measure may be a prohibition from opening or maintaining a correspondent account in the United States for, or on behalf of, the Specified Banks. In that case, Alpine will take the following steps:

(1) The AML Officer or designee will review our account records, including correspondent account records, to ensure that our accountholders and correspondent accountholders maintain no accounts directly for, or on behalf of, the Specified Banks; and

(2) Alpine will apply due diligence procedures to our correspondent accounts that are reasonably designed to guard against indirect use of those accounts by the Specified Banks.

• Notification to Correspondent Accountholders

Alpine will notify our correspondent accountholders that the account may not be used to provide the Specified Banks with access to us. Ultimately, Alpine has flexibility in determining the language used in the sample notification language. For example, Alpine may use the following sample language, but is not limited in using the specific language detailed below:

"*Notice*: Pursuant to U.S. regulations issued under section 311 of the USA

PATRIOT Act, 31 CFR 103.192, we are prohibited from opening or maintaining a

correspondent account for, or on behalf of, [the Specified Banks]. The regulations also require us to notify you that your correspondent account with our financial institution may not be used to provide [the Specified Banks] with access to our financial institution. If we become aware that [the Specified Banks] are indirectly using the correspondent account you hold at our financial institution, we will be required to take appropriate steps to prevent such access, including terminating your account."

Alpine will transmit a one-time notice to our correspondent accounts by mail, fax or email, or including the information in the next regularly occurring transmittal to correspondent accountholders and document our compliance with the notification requirement.

• Identification of Indirect Use

Alpine will take reasonable steps in order to identify any indirect use of our correspondent accounts by the Specified Banks. We will determine if such indirect use is occurring from transactional records that we maintain in the normal course of business. We will take a risk-based approach when deciding what, if any, additional due diligence measures we should adopt to guard against the indirect use of correspondent accounts by the Specified Banks, based on risk factors such as the type of services offered by, and geographic locations of, their correspondents.

Alpine understands its ongoing obligation to take reasonable steps to identify all correspondent account services our correspondent accountholders may directly or indirectly provide to the Specified Banks.

9.11 Detecting Potential Money Laundering

Responsibility	• AML Officer or designee • Other designated supervisor(s) for review of AML Officer accounts • All other employees
Resources	• Internal reports of transactions, available exception reports • Performance of tasks and other duties, typically handled as part of routine work
Frequency	• As required
Action	All: • Review reports of transactions (cash and security transactions) to identify potential

	money laundering (including employee accounts) , including the AML Officer's accounts • Review daily reports and identify potentially suspicious activity • Report suspicious activity (see the policy in this chapter) AML Officer or designee: • Notify RRs, supervisors, and close accounts, in consultation with business unit leaders, when necessary
Record	• Reports reviewed • Action taken, when necessary • Suspicious activity reports and supporting documentation

Alpine has an ongoing program to identify potential money laundering. Monitoring will be conducted using available exception reports or reviews of other reports of account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as "non-cooperative" are involved, or involve "red flags" (indicators of potential money laundering) which are included in the *Money Laundering* policy in the chapter *GENERAL EMPLOYEE POLICIES*. Items reviewed include trading and wire transfer transactions in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that customer. Among the information used to determine whether to file a suspicious activity report are exception or transaction reports that include transaction size, location, type, number, and nature of the activity.

9.11.1 Alpine's Employee Reporting Obligations

Alpine has included an educational policy *(Money Laundering)* in the chapter *GENERAL EMPLOYEE POLICIES* to educate employees on money laundering and guidelines for detecting money laundering activities. Periodic detection of money laundering and the obligation to report suspicious activities will be included in continuing education and other educational programs for employees.

All employees are obligated to promptly report to the AML Officer or designee any known or suspected violations of anti-money laundering policies as well as other suspected violations or crimes. If the potential violation implicates the AML Officer, it should be reported to a senior officer of Alpine. All reports are confidential and the employee will suffer no retaliation for making them.

What to report: Crimes or suspected crimes by individuals (whether associated with Alpine, a customer, or prospective customer) are required to be reported. This includes suspicion that Alpine is being used as a conduit for criminal activity such as money laundering or structuring transactions (discussed below) to evade the BSA reporting requirements. There is no clear definition of what constitutes a "crime." If you believe some improper or illegal activity is occurring, it is your obligation to be attentive and alert to the red flags and report to the AML Officer or designee any new or existing customers who may be engaged in potential violations of anti-money laundering regulations.

SAR reports: By law, Alpine and its employees cannot disclose to the customer or anyone other than authorized parties that it has filed a SAR or provide information that would reveal the existence of a SAR. Questions regarding SAR filings should be referred to Compliance. If you become aware of an unauthorized disclosure of an SAR or you receive a subpoena for an SAR, **immediately contact the Compliance Department**. Designated Compliance personnel will be responsible for contacting FINCEN to report the unauthorized disclosure.

9.11.2 Role Of Operations Personnel

Operations personnel are an important first line of defense in preventing transactions with sanctioned parties. The following guidance is provided to assist Operations personnel in identifying blocked parties. Any questioned accounts or transactions should be referred to the AML Officer or designee.

- On a monthly basis, the AML Officer or designee shall provide a current list of countries included on the OFAC list. These are countries considered potential havens for money laundering, drug trafficking, or terrorist activities. Information is included on the OFAC web site at www.treas.gov/ofac.
- On a periodic basis, the AML Officer or designee shall provide a current list of countries included on the Financial Action Task Force (FATF) list. The Financial Action Task Force (FATF) is the global standard setting body for anti-money laundering and combating the financing of terrorism. In order to protect the international financial system from money laundering and financing of terrorism risks and to encourage greater compliance with their standards, the FATF identified jurisdictions that have strategic deficiencies and works with them to address those deficiencies that pose a risk to the international financial system.
- When processing the opening of accounts, Operations employees shall determine if new accounts have addresses as residents of countries included on the OFAC list and report any that appear on the list to the AML Officer or designee.
- Questions regarding requests to transfer funds or securities to residents or entities domiciled in any country included on the OFAC list shall be reported to the AML Officer or designee.

9.11.3 Role of Retail Brokerage Personnel

Retail sales personnel are also an important first line of defense in identifying, detecting and/or preventing transactions. Retail sales personnel are in a unique position of knowing the client best. It is important that you understand the customer's financial resources, business activities, and sources of funds to identify when purported or actual activity deviates from the standard transactions one expects to see in a customer account. The process of knowing the customer does not end at the time the account established. The process of knowing the customer continues through the ongoing maintenance of the client's account. Any questioned accounts or transactions should be referred to the AML Officer or designee.

9.11.4 Monitoring Accounts for Suspicious Activity

Rules/Resources: USA PATRIOT Act Sec. 356; FinCEN Guidance on Suspicious Activity Report Supporting Documentation: http://www.fincen.gov/Supporting_Documentation_Guidance.pdf; FinCEN Guidance FIN-2008-G005

Responsibility	• AML Officer or designee
Resources	• Reports from employees of crimes or suspected crimes • Suspicious activities detected through ongoing reviews • Other available information
Frequency	• As required
Action	• Review and investigate suspicious transactions referred by employees • Determine whether Alpine will file a SAR • If appropriate, file Form SAR-SF with FinCEN and state authorities • Notify senior management, as appropriate, of forms filed
Record	• Notes and other documented reviews are retained in a suspicious activity file • Copies of SARs filed by Alpine are retained in the SAR file with notation of when and to whom sent

Alpine will file Suspicious Activity Reports (SARs) for transactions that may be indicative of money laundering activity. Suspicious activities include a wide range of questionable activities. Examples may include, but are not limited to, trading that constitutes a substantial portion of all trading for the day in a particular security; trading or journaling between/among accounts, particularly between related owners; late day trading; heavy trading in low-priced securities; unexplained wire transfers, including those to known tax havens; unusually large deposits of funds or securities; shares of physical securities of low-priced securities that have an issue date of less than 12 months and are more than one million shares or have a market value over a certain amount.

Determining whether an activity or series of activities is suspicious is a facts and circumstance analysis and will be made by the AML Officer or designee.

Alpine will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business. (Red flags are identified below.) Alpine will conduct the following reviews of activity that our monitoring system detects:

Report Name	Report Description
OFAC Report	This report is used to identify potential matches between the OFAC SDN List and the customer/prospective customer.
Accounts in Non-Cooperative countries	This report compares the account holder's address against the FATF list of non-cooperative countries to screen for matches.
Foreign Account Activity	This report lists all Cash Movements or ACH activities in accounts not associated to the US or USA.
Account Activity in Non-Cooperative and Blocked Countries	This report displays any trade activity for accounts with addresses in non-cooperative or blocked countries for the previous business day.
Foreign Correspondents	This report lists all foreign correspondent banks to comply with PATRIOT Act sections 312, 313, and 319(b).
Currency Activity $5K or greater	This report lists all cash movements or ACH activities between $5,000 and $1,000,000.
Transmittal Activity	This report/query lists all transmittal activity.
Trade Blotters	This report lists all trading activity.

The AML Officer or designee will document our monitoring and reviews as follows:

- Denote the review date, reviewer name (or initial or signature) and action taken on the electronic or paper report; or
- Other format as authorized by the AML Officer or designee.

The AML Officer or designee will conduct an appropriate investigation and review relevant information from internal or third-party sources before a SAR-SF is filed which is further discussed in the section titled "Responding to Red Flags and Suspicious Activity".

The AML Officer or designee will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

9.11.5 Emergency Notification to Law Enforcement by Telephone

Rules/Resources: FINRA Notice to Members 02-21

In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, the AML Officer or designee will immediately call an appropriate law enforcement authority. If a customer or company appears on OFAC's SDN list, the AML Officer or designee will call the OFAC Hotline at (800) 540-6322. Other contact numbers Alpine will use are: FinCEN's Financial Institutions Hotline (866- 556-3974) (especially to report transactions relating to terrorist activity), local U.S. Attorney's office (801-524-5682), local FBI office (*801-579-1400)* and local SEC office (801-524-5796*)* (to voluntarily report such violations to the SEC in addition to contacting the appropriate law enforcement authority). If Alpine notify the appropriate law enforcement authority of any such activity, Alpine must still file a timely SAR-SF.

Although Alpine is not required to, in cases where we have filed a SAR-SF that may require immediate attention by the SEC, we may contact the SEC via the SEC SAR Alert Message Line at (202) 551-SARS (7277) to alert the SEC about the filing. Alpine understands that calling the SEC SAR Alert Message Line does not alleviate our obligations to file a SAR-SF or notify an appropriate law enforcement authority.

9.11.6 Potential Red Flags

Rules/Resources: NASD Notice to Members 02-21

The following are examples of risk indicators (red flags) that may suggest potential money laundering. This is not an all-inclusive list.

Red Flags indicating potential Money Laundering
Customers – Insufficient or Suspicious Information
The customer exhibits unusual concern regarding Alpine's compliance with government reporting requirements and Alpine's AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents that cannot readily be verified.
The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business strategy.
The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
The customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets, when requested.
The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
Customer appears reluctant to provide complete information about nature and purpose of business,

officers and directors or business location.
Customer has no discernable reason for utilizing the firm's services.
Efforts to Avoid Reporting and Recordkeeping
Customer attempts to persuade an employee not to file required reports or not to maintain required records.
Customer is reluctant to provide information needed to file reports or fails to proceed with a transaction when information is requested.
Customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
Certain Funds Transfer Activities
The customer engages in activity involving the practice of depositing penny stocks, liquidating them, and wiring proceeds. A request to liquidate shares may also represent engaging in an unregistered distribution of penny stocks which may also be a red flag. [FINRA Regulatory Notice 09-05]
The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from Alpine's policies relating to the deposit of cash and cash equivalents.
The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force (FATF).
The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
The customer's account shows numerous currency or cashier's check transactions aggregating to significant sums.
The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven
The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
The customer makes a funds deposit for the purpose of

purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.
The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
The customer requests that a transaction be processed in such a manner to avoid Alpine's normal documentation requirements.
Certain Deposits or Dispositions of Physical Certificates
Physical certificate is titled differently than the account.
Physical certificate does not bear restrictive legend, but based on history of the stock and/or volume of shares trading, it should have such a legend.
Customer's explanation of how he or she acquired the certificate does not make sense or changes.
Customer deposits the certificate with a request to journal the shares to multiple accounts, or to sell or otherwise transfer ownership of the shares.
Certain Securities Transactions
The customer, for no apparent reason or in conjunction with other "red flags," engages in transactions involving certain types of securities, such as penny stocks, Regulation "S" (Reg S) stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.
The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent business purpose or other purpose.
The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.
Customer journals securities between unrelated accounts for no apparent business reason.
Customer engages in prearranged or other non-competitive trading, including wash or cross trades of illiquid securities.
The entering of a sell (or buy) order by a client knowing that a corresponding buy (or sell) order of substantially the same size, at substantially the same time and at substantially the same price has been or will be entered by another client.
Trades by single clients or clients trading in coordination that consists of large percentages of the securities volume.
Parties that use algorithms to trade in a particular security by placing and then cancelling layers of orders in that security, creating fluctuations in the national best bid or offer of that security, increasing order book depth and using the non-bona fide orders to send false

signals regarding the demand for such security, which the algorithms misinterpreted as reflecting sincere demand. Layering orders are intended to deceive certain algorithms into buying (or Selling) stocks from (or to) the layering traders bona fide trade at prices that are artificially raised (or lowered) by the layering trader.
Customer's trading patterns suggest that he or she may have inside information.
Transactions Involving Penny Stock Companies
Company has no business, no revenues and no product
Company has experienced frequent or continuous changes in business structure.
Officers or insiders of the issuer are associated with multiple penny stock issuers.
Company undergoes frequent material changes in business strategy or its line of business.
Officers or insiders of the issuer have a history of securities violations.
Company has not made disclosures in SEC or other regulatory filings.
Company has been the subject of a prior trade suspension.
Other Suspicious Customer Activity
Funds deposits for purchase of a long-term investment followed shortly by a request to liquid the position and transfer proceeds out of the account.
Law enforcement subpoenas.
Large number of securities transactions across a number of jurisdictions.
Buying and selling securities with no purpose or in unusual circumstances (*e.g.* churning at customer's request).
Payment by third-party check or money transfer without an apparent connection to the customer.
Payments to third-party without apparent connection to customer.

In view of the risk factors listed in the section titled "Potential Red Flags" as well as perhaps other circumstances, Alpine frequently conducts additional inquiries to determine whether filing a SAR is warranted. Further, as part of its efforts to review the proposed resale of restricted or control securities, Alpine frequently gains additional information about its customer or proposed securities transactions. Additional investigation may either heighten Alpine's suspicions about activity or demonstrate that initial concerns are not confirmed and that the subject person's proposed activities appear legal, reasonable, and for a legitimate business purpose when all of the circumstances are considered as a whole. Where such further inquiry demonstrates that filing a SAR is warranted, it is Alpine's policy to do so. Similarly, in some circumstances stock may be tendered in circumstances that suggest or make one suspicious that the proposed resale may be part of a scheme to illegally distribute stock without registration (e.g. Section 5 violations). In those circumstances, Alpine would ordinarily file an SAR. Conversely, when such further investigations overcome the initial suspicions or risk factors and suggest that the proposed activities or transactions are legal, reasonable, and for a legitimate business purpose, Alpine will not file a SAR.

9.11.6.1 Potential Red Flags cont.d

In view of the risk factors listed in the section titled "Potential Red Flags" as well as perhaps other circumstances, Alpine frequently conducts additional inquiries to determine whether filing a SAR is warranted. Further, as part of its efforts to review the proposed resale of restricted or control securities, Alpine frequently gains additional information about its customer or proposed securities transactions. Additional investigation may either heighten Alpine's suspicions about activity or demonstrate that initial concerns are not confirmed and that the subject person's proposed activities appear legal, reasonable, and for a legitimate business purpose when all of the circumstances are considered as a whole. Where such further inquiry demonstrates that filing a SAR is warranted, it is Alpine's policy to do so. Similarly, in some circumstances stock may be tendered in circumstances that suggest or make one suspicious that the proposed resale may be part of a scheme to illegally distribute stock without registration (e.g. Section 5 violations). In those circumstances, Alpine would ordinarily file an SAR. Conversely, when such further investigations overcome the initial suspicions or risk factors and suggest that the proposed activities or transactions are legal, reasonable, and for a legitimate business purpose, Alpine will not file a SAR.

9.11.6.2 Circumstances In Which A SAR May Not Be Filed

The following circumstances, intended to be illustrative and not exhaustive, tend to suggest that initial suspicions may not warrant filing a SAR.

- A foreign customer provides evidence respecting the legitimacy of the source of the funds or securities deposited with Alpine as part of regular, common business activity, such as investing in restricted securities.
- Multiple transaction in securities result from contractual limitations for resales or a person's desire to limit negative market impacts.
- Several investors in a single issuer seek to liquidate their securities acquired to provide legitimate financing to such issuer.
- Offshore accounts are held in jurisdictions that are not identified by the Financial Action Task Force as maintaining an inadequate AML/CFT regime.
- Customers provide information requested even though the accounts are maintained in jurisdictions where local laws, regulations, or provisions (such as privacy laws) prevent or limit the collection of client identification information.
- Customers are not senior political or government officials ("politically exposed persons") of a foreign government.
- Customers that are closely held corporations, partnerships, limited liability companies or similar entities appear to have been formed for legitimate and lawful purposes.
- Entities that appear to be engaged in some sort of financial services or investment activities appear properly licensed in their home jurisdiction.
- Customers who are non-resident aliens have legitimate business activities and purposes.
- Entities are willing to disclose their beneficial owners and the persons who own the securities beneficially.
- Securities issued by foreign investment funds or other issuers are engaged in legitimate activities and do not appear to provide financing to sanctioned governments or parties.
- Foreign securities are issued in registered, as opposed to bearer, form.
- Transparent ownership, control, and activities.
- Full identification (i.e., passport or similar photo identification) of principals and beneficial owners.
- Transactions in recognized financial markets.
- Fully disclosed details about accounts or proposed activities, notwithstanding the availability of local privacy or information shield laws.

In some circumstances customers tender restricted stock for public resale without restriction that, upon investigation and review, does not appear eligible for resale. In the absence of special incriminating circumstances such as evidence of part of a larger scheme to illegally distribute stock without registration, the fact that Alpine determines that the stock is not currently eligible for resale without registration is not deemed to

warrant filing an SAR. Requests for other Alpine action that it ultimately determines not to effect are considered similarly and treated similarly with respect to not filing a SAR.

9.11.6.3 Exclusions from SAR Filing

The AML Officer or designee is not required to file a SAR involving violations otherwise reported to law enforcement authorities such as:

- a robbery or burglary that is reported to law enforcement authorities
- lost, missing, counterfeit, or stolen securities reported pursuant to 17f-1
- a violation of federal securities laws or SRO rules by Alpine, its officers, directors, employees, or RRs that are reported to the SEC or SRO, except for violations of Rule17a-8 (filing of Currency and Transaction Reports) which must be reported on a SAR

9.11.6.4 Responding to Red Flags and Suspicious Activity

When an Alpine employee detects any red flag, or other activity that may be suspicious, the employee must notify the AML Officer or designee. Under the direction of the AML Officer or designee, Alpine will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or filing a SAR-SF.

9.11.6.5 Identifying Potential Suspicious Activity

Alpine uses a number of tools to identify potential suspicious activity including:

- Transaction information including disbursement of funds or securities are reviewed periodically by the OSJ Branch Manager and Trading personnel (as it relates to trading activity) and AML Officer or their designees.
- The AML Officer or designee provides education to Alpine's RR, to Supervisors approving new accounts, operations personnel and to the OSJ Branch Manager.
- Employee reports of potential suspicious activity are given to the AML Officer or designee.
- It is always at the AML Officer's (or designee's) discretion, when taking into consideration all factors, when a SAR should be filed.

All employees have an ongoing obligation to report potentially suspicious activity to the AML Officer or designee.

9.11.6.6 Suspicious Transactions and BSA Reporting

9.11.6.6.1 Filing A SAR

Alpine will file SAR-SFs with FinCEN for any transactions (including deposits and transfers) conducted or attempted by, at or through our firm involving $5,000 or more of funds or other assets (either individually or in the aggregate) where Alpine knows, suspects, or has reason to suspect:

- The transaction involves funds derived from illegal activity or intended or conducted to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation.
- the transaction is designed, whether through structuring or other means, to evade the requirements of the Bank Secrecy Act (BSA).
- The transaction has no business or apparent lawful purpose or is not in which the customer would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, Alpine knows of no reasonable explanation for the transaction, or
- The transaction involves the use of Alpine to facilitate criminal activity.

9.11.6.6.2 SAR Filing Deadlines

The AML Officer or designee will report suspicious transactions by completing a SAR-SF, and will collect and maintain supporting documentation as required by the BSA regulations. The AML Officer or designee will file a SAR-SF no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR-SF. If no suspect is identified on the date of initial detection, we may delay filing the SAR-SF for an additional 30 calendar days pending identification of a suspect, but in no case will the reporting be delayed more than 60 calendar days after the date of initial detection. The phrase "initial detection" does not mean the moment a transaction is highlighted for review. The 30-day (or 60-day) period begins when an appropriate review is conducted and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR requirements. A review should be initiated promptly upon identification of unusual activity that warrants investigation.

9.11.6.7 Currency Transaction Reporting

Rules/Resources: SEC Securities Exchange Act of 1934 Rule 17a-8; Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart C; FinCEN pamphlet on CTR reporting: http://www.fincen.gov/whatsnew/html/20090224.html]

9.11.6.7.1 Definitions

"Currency" is defined as the coin and paper money of the U.S. or legal tender of other countries. Currency also includes U.S. silver certificates, U.S. notes, federal reserve notes, and official foreign bank notes customarily used and accepted as a medium of exchange in a foreign country.

The Bank Secrecy Act requires broker-dealers to report certain transactions relating to currency transactions, as follows:

- Report cash or currency deposits of more than $10,000, including multiple deposits on the same day that would total more than $10,000. A currency Transaction Report (CTR) is filed with the Financial Crimes Enforcement Network (FinCEN), a bureau of the Treasury Department. Some state regulators also require reporting of currency transactions.
- Report currency or bearer instruments over $10,000 transferred into or out of the U.S. The Currency and Monetary Instrument Transportation Report (CMIR) is filed with the U.S. Customs Service.

The following summarizes the reporting requirements under the Bank Secrecy Act. Alpine's CFO or designee is responsible for maintaining records of any currency reports required to be filed by Alpine and retaining them for five years.

9.11.6.7.2 Transactions Involving Currency Over $10,000

If Alpine accepts a currency deposit exceeding $10,000, it is required to file a Currency Transaction Report (CTR) with the Financial Crimes Enforcement Network (FinCEN). Multiple transactions by the same person equaling over $10,000 in any one day must also be reported. Alpine's COO or designee is responsible for filing these reports and maintaining records of them for a period of five years from the filing date.

Operations personnel are responsible for receiving currency and will process these requests in accordance with their standard operating procedures. Currency deposits in the amount greater than $10,000 will be reported to the AML Officer or designee. Multiple transactions by the same person equaling over $10,000 in any one day must also be reported to the AML Officer or designee. The AML Officer or designee will notify Alpine's COO or designee to complete the required filings.

9.11.6.8 Currency and Monetary Instrument Transportation Reports (CMIR)

Broker-dealers are required to file a Currency and Monetary Instrument Transportation Report (CMIR) with the U.S. Customs Service to report transactions in physical currency and/or bearer instruments which alone or in combination exceed $10,000 and which are shipped or transported into or outside the U.S. This filing is not required for currency or other monetary instruments mailed or shipped through the postal service or by common

carrier. Alpine's COO or designee is responsible for filing these reports and maintaining these records for the required retention period. Refer to the section titled "Recordkeeping Requirements" for more information. The COO or designee will file a CMIR with the Commissioner of Customs if we discover that we have received or caused or attempted to receive from outside of the U.S. currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time (on one calendar day or, if for the purposes of evading reporting requirements, on one or more days). The COO or designee will also file a CMIR if we discover that we have physically transported, mailed or shipped or caused or attempted to physically transport, mail or ship by any means other than through the postal service or by common carrier currency or other monetary instruments of more than $10,000 at one time (on one calendar day or, if for the purpose of evading the reporting requirements, on one or more days). Alpine will use the CMIR Form provided on FinCEN's Web site.

9.11.6.9 Prohibition Against Structuring Deposits To Avoid Reporting

Cash or currency deposits or attempted deposits which appear to be part of a deposit structure to avoid IRS or Customs currency reporting requirements or Alpine's limitations, or are otherwise suspicious, may not be accepted and must be reported to the OSJ Branch Manager. Employees are prohibited from:

- aiding or advising a customer in structuring a transaction to avoid reporting requirements
- holding instruments for deposit on succeeding days
- transporting cash or cash equivalents or bearer instruments to a bank on behalf of a customer

9.11.6.10 State Reporting Requirements

States have adopted various currency and suspicious activity reporting requirements. Most states have entered into an agreement with FinCEN to provide them with duplicate copies of forms filed by broker-dealers. Some states, however, require duplicate filing with the states themselves at the time the broker-dealer files with a federal agency. Alpine's CFO or designee will file reports as required under state requirements.

9.11.6.11 Foreign Financial Account Reporting Requirements And Recordkeeping (FBAR)

Rules/Resources: Bank Secrecy Act 31 CFR Chapter X Part 1010 Subpart C; Form: http://www.fincen.gov/forms/files/f9022-1_fbar.pdf; FinCEN Notice 2012-1

Certain "United States persons" that maintain accounts (including any account where the person has a financial interest in, or signature or other authority over) in foreign jurisdictions and with aggregate balances exceeding $10,000 are required to file a Report of Foreign Bank and Financial Accounts (FBAR) Department of Treasury Form 90-22.1 with FinCEN on or before June 30th of each calendar year for accounts maintained during the previous calendar year. Certain U.S. persons with signature authority over, but no financial interest in, foreign financial accounts of their employers and entities related to their employers have an extension until June 30, 2013 to file Form 90-22.1 (see FinCEN Notice 2012-1). The FINOP or designee is responsible for filing the annual report if it is required for Alpine.

The filing requirement applies to:

- Non-resident aliens and foreign entities "in and doing business" in the U.S.
- All forms of U.S. business entities, trusts, estates with foreign accounts.
- U.S. citizens and residents with signature or other authority over a foreign account.
- Trust beneficiaries with a greater than 50% beneficial interest in a trust with a foreign account.
- U.S. citizens and resident stockholders with greater than 50% of the value or vote of the shares of a corporation with foreign accounts.
- Entities that are disregarded for tax purposes, such as limited liability companies.

The filing requirement does not apply to certain entities or situations. The regulation should be consulted for specific exemptions or conditions of exemptions.

- If the account is maintained in the United States, it is not considered a foreign account even if it holds foreign assets.
- An omnibus account held by a custody bank that holds assets both in the U.S. and outside the U.S. is not considered a foreign account unless the customer has direct access to its foreign holdings maintained at the foreign institution.
- Certain entities are excluded including: foreign hedge funds, venture capital funds, or private equity funds; tax-exempt investors that own offshore "blocker corporations;" government pension funds; pension plan participants and IRA owners (provided the trustee files a FBAR); investment advisers and employees of such advisers that provide advice to SEC-registered entities; remainder interests in trusts and beneficiaries of discretionary trusts; employees of a U.S. or foreign entity that issued a class of foreign equity (including ADRs) registered with the SEC.

There also are exemptions for officers or employees with signature or other authority over certain foreign financial accounts but no financial interest in the reportable account. The regulation should be consulted for details regarding who is not required to notify FinCEN regarding signature or other authority over such an account.

9.11.6.12 Monetary Instrument Purchases

Rules/Resources: 31 C.F.R. § 103.29. See also 31 C.F.R. 103.22(b), 52 Fed. Reg. 52250 (October 17, 1994) (Final Rule Amendments to BSA Regulations Relating to Identification Required to Purchase Bank Checks and Drafts, Cashier's Checks, Money Orders, and Traveler's Checks).

Alpine does not issue bank checks or drafts, cashier's checks, money orders or traveler's checks in the amount of $3,000 or more.

9.11.6.13 Fund Transmittals of $3,000 or More Under the Travel Rule

Rules/Resources: Bank Secrecy Act 31 CFR Chapter X Part 1010 Subpart D; FINRA Notice to Members 97-13, 96-67 and 95-69; SEC Q&As: http://www.sec.gov/about/offices/ocie/aml2007/fincen-advissu7.pdf; SEC Q&As: http://www.sec.gov/about/offices/ocie/aml2007/fincen-advsiii.pdf

When Alpine is the transmittor's financial institution in funds of $3,000 or more for domestic and international funds transfers (including wire fund transfers), Alpine will retain either the original or a copy (*e.g.*, microfilm, electronic record) of the transmittal order. Alpine will also record on the transmittal order the following information: (1) the name and address of the transmitter; (2) if the payment is ordered from an account, the account number; (3) the amount of the transmittal order; (4) the execution date of the transmittal order; and (5) the identity of the recipient's financial institution. In addition, Alpine will include on the transmittal order as many of the following items of information as are received with the transmittal order: (1) the name and address of the recipient; (2) the account number of the recipient; (3) any other specific identifier of the recipient; and (4) any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order.

Alpine is not required to retain this information if it involves transfers between accounts that are not for the same owner and transfers to third parties including banks and other financial institutions.

Alpine will also verify the identity of the person placing the transmittal order (if we are the transmitting firm), provided the transmittal order is placed in person and the transmitter is not an established customer of the firm (*i.e.*, a customer of the firm who has not previously maintained an account with us or for whom we have not obtained and maintained a file with the customer's name, address, taxpayer identification number, or, if none, alien identification number or passport number and country of issuance). If a transmitter or recipient is conducting business in person, Alpine will obtain:

1. the person's name and address;
2. the type of identification reviewed and the number of the identification document (*e.g.*, driver's license); and

3. the person's taxpayer identification number (*e.g.,* Social Security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record the lack thereof.

If a transmitter or recipient is not conducting business in person, Alpine will obtain the person's name, address, and a copy or record of the method of payment (*e.g.,* check or credit card transaction). In the case of transmitters only, Alpine will also obtain the transmitter's taxpayer identification number (*e.g.,* Social Security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof. In the case of recipients only, Alpine will obtain the name and address of the person to which the transmittal was sent.

Records of transfers are available for inspection by regulators and other appropriate authorities, when requested.

9.11.6.14 Foreign Currency Transactions

Foreign financial institutions may purchase U.S.-denominated bonds, generally issued by foreign governments, with the local currency, which are then transferred to a U.S. broker-dealer and sold, with proceeds then transferred offshore. U.S. broker-dealers act as intermediaries in these transactions and may receive foreign bonds or other securities worth millions of U. S. dollars without knowing who or how many underlying customers may be involved. RRs and Alpine must be diligent about such transactions which may involve money laundering.

9.11.7 AML Recordkeeping Requirements

Rules/Resources: Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart D

a. **Responsibility for Required AML Records and SAR-SF Filing**

Alpine's AML Officer or designee is responsible for ensuring that SAR-SFs are filed as required and retaining all related documentation for a period of five years from the filing date. Each of the parties responsible for filing the CTRs, CMIRs, FBARs and relevant documentation on customer identity and verification and funds transmittals will be responsible for ensuring that such records are maintained properly at least five years from the filing date. Alpine will keep other documents according to existing BSA and other recordkeeping requirements, including certain SEC rules that require six-year retention periods (*e.g.*, Exchange Act Rule 17a-4(a) requiring firms to preserve for a period of not less than six years, all records required to be retained by Exchange Act Rule 17a-3(a)(1)-(3), (a)(5), and (a)(21)-(22) and Exchange Act Rule 17a-4(e)(5) requiring firms to retain for six years account record information required pursuant to Exchange Act Rule 17a-3(a)(17)).

b. **SAR-SF Maintenance and Confidentiality**

Alpine will hold SAR-SFs and any supporting documentation confidential. Alpine will not inform anyone outside of FinCEN, the SEC, an SRO registered with the SEC or other appropriate law enforcement or regulatory agency about a SAR-SF. Alpine will refuse any subpoena requests for SAR-SFs or for information that would disclose that a SAR-SF has been prepared or filed and immediately notify FinCEN of any such subpoena requests that we receive. Alpine will segregate SAR-SF filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR-SF filings. Our AML Officer or designee will handle all subpoenas or other requests for SAR-SFs. Alpine may share information with another financial institution about suspicious transactions in order to determine whether Alpine will jointly file a SAR according to the provisions set forth elsewhere in this Policy. In cases in which Alpine file a joint SAR for a transaction that has been handled both by us and another financial institution, both financial institutions will maintain a copy of the filed SAR.

i. **Providing SARs Information To SROs**

Rules/Resources: SEC letter to CEOs: http://www.sec.gov/about/offices/ocie/brokerdealerletter.htm

While SARs are to be treated as confidential, Alpine will provide SARs and supporting documentation available to any self-regulatory organization (SRO) that examines Alpine for compliance with the SAR Rule, as requested by the SEC (see SEC letter to CEOs referenced above). The request may be part of a routine examination, an investigation, or part of the SRO's risk assessment effort within its examination program.

ii. Prohibition Against Disclosure

By statute and regulation, Alpine may not inform customers or third parties that a transaction has been reported as suspicious. U.S. Treasury and Federal Reserve Board regulations also require Alpine to decline to produce SARs in response to subpoenas and to report to FinCEN and the Federal Reserve Board the receipt of such requests and Alpine's response. Failure to maintain the confidentiality of SARs may subject an employee to civil and criminal penalties under Federal law. Violations may be enforced through civil penalties of up to $100,000 for each violation and criminal penalties of up to $250,000 and/or imprisonment not to exceed five years. Alpine may also be liable for civil money penalties resulting from AML deficiencies that led to improper SAR disclosure up to $25,000 per day for each day the violation continues.

Procedures to protect the confidentiality of SARs may include, but not be limited to, the following:

- Access to SARs is limited to employees on a "need-to-know" basis
- SARs may be maintained in locked physical or contained to electronic files
- SARs may not be left on desks or on open computer files and may not be viewed by unauthorized persons
- SARs shared with others will be clearly marked "Confidential"

The CCO or designee (or Alpine's legal department) is responsible for responding to subpoena requests and the AML Officer or designee for will notify FinCEN and our primary federal regulator, where required by law.

iii. Recipient of an Unauthorized SAR Disclosure

If you become aware of an unauthorized disclosure of a SAR or if you receive a subpoena request for a SAR, immediately contact the Compliance Department. Compliance will contact FINCEN's Office of Chief Counsel at (703) 905-3590. Alpine may also be required to contact our primary federal regulator.

c. Additional Records

Rules/Resources: Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart D 1023.410

Alpine shall retain either the original or a microfilm or other copy or reproduction of each of the following:

- A record of each extension of credit in an amount in excess of $10,000, except an extension of credit secured by an interest in real property. The record shall contain the name and address of the person to whom the extension of credit is made, the amount thereof, the nature or purpose thereof and the date thereof;
- A record of each advice, request or instruction received or given regarding any transaction resulting (or intended to result and later canceled if such a record is normally made) in the transfer of currency or other monetary instruments, funds, checks, investment securities or credit, of more than $10,000 to or from any person, account or place outside the U.S.;
- A record of each advice, request or instruction given to another financial institution (which includes broker-dealers) or other person located within or without the U.S., regarding a transaction intended to result in the transfer of funds, or of currency, other monetary instruments, checks, investment securities or credit, of more than $10,000 to a person, account or place outside the U.S.;
- Each document granting signature or trading authority over each customer's account;
- Each record described in Exchange Act Rule 17a-3(a): (1) (blotters), (2) (ledgers for assets and liabilities, income, and expense and capital accounts), (3) (ledgers for cash and margin accounts), (4) (securities log), (5) (ledgers for securities in transfer, dividends and interest received, and securities borrowed and loaned), (6) (order tickets), (7) (purchase and sale tickets), (8) (confirms), and (9) (identity of owners of cash and margin accounts);

- A record of each remittance or transfer of funds, or of currency, checks, other monetary instruments, investment securities or credit, of more than $10,000 to a person, account or place, outside the U.S.; and
- A record of each receipt of currency, other monetary instruments, checks or investment securities and of each transfer of funds or credit, of more than $10,000 received on any one occasion directly and not through a domestic financial institution, from any person, account or place outside the U.S.

9.12 Clearing/Introducing Firm Relationships

Rules/Resources: 31 CFR 103.110; FINRA Rule 3310, NASD Rule 3230, FIN-2006-G003: Frequently Asked Questions: Foreign Bank Recertifications under 31 C.F.R. § 103.77 (February 3, 2006).

Alpine will exchange information, records, data and exception reports as necessary to comply with our contractual obligations and with AML laws.

In our clearing agreements, Alpine has addressed how Alpine and each correspondent firm will apportion customer and transaction functions and how we will share information. Alpine understands that the apportionment of functions will not relieve either of us from our independent obligation to comply with AML laws, except as specifically allowed under the BSA and its implementing regulations.

9.13 Training Programs

Rules/Resources: FINRA Rule 3310, See NTM 02-21, FinCEN SAR Narrative Guidance Package (11/2003), FinCEN Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting (10/10/2007)

Alpine will develop ongoing employee training under the leadership of the AML Officer or designee with input from senior management. This training may be developed in-house or Alpine may engage the services of an online training vendor or utilize other media such as educational pamphlets, videos, explanatory memos. This training will occur on at least an annual basis and will be based on our firm's size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law. The AML Officer or designee will maintain records to show the persons trained, the dates of training and the subject matter of their training. The AML Officer or designee reserves the right to require specialized training for certain groups within Alpine, such as Operations, Compliance, Retail sales, etc.

Our training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of SAR-SFs); (3) what employees' roles are in the firm's compliance efforts and how to perform them; (4) the firm's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the BSA

9.14 Independent Testing, Evaluation and Reporting

Rules/Resources: FINRA Rule 3310.01

Responsibility	• AML Officer or designee
Resources	• Policies and procedures • Independent testing results
Frequency	• Annual - schedule, conduct, and follow up testing (unless firm qualifies for testing every two years)

Action	• Identify person(s) to conduct testing • Conduct testing • Report results to CEO in annual compliance report • Revise policies and procedures as necessary • Conduct follow-up to determine corrective action has been taken
Record	• Independent testing results including who conducted and dates of review • Report to CEO • Record of changes to policies and procedures resulting from testing • Record of follow-up actions

The AML Officer or designee will be responsible for an annual (on a calendar-year basis) independent testing of Alpine's policies and procedures regarding money laundering and the effectiveness of the program, as described in this chapter. The tests performed will be either by an employee of Alpine, if such employee qualifies pursuant to the SRO rules for independence set forth below, or by a qualified non-employee, third party. At the discretion of Alpine's Board of Directors, the AML Officer or designee may be directed to conduct interim testing of Alpine's policies and procedures regarding money laundering and the effectiveness of the program, if they believe such interim tests are warranted.

SRO rules require that the person(s) conducting the independent testing of Alpine's AML program:

- is not the AML Officer
- is not performing any AML procedures that are being tested and reviewed
- is not an individual who is supervised by or otherwise reports to the AML Officer or to someone who performs any AML procedures
- is knowledgeable regarding the Bank Secrecy Act, money laundering activities and related regulations

After Alpine has completed the independent testing, the AML Officer or designee will report its findings to senior management. Alpine, under the leadership of the Executive Team will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

9.15 Monitoring Employee Conduct and Accounts Programs

Alpine will subject employee accounts to the same AML procedures as customer accounts, as noted elsewhere in Alpine's written supervisory procedures. Provisions for the review of the AML Officer or designee's personal accounts are also addressed elsewhere in Alpine's written supervisory procedures. Please refer to the section titled "Employee and Employee Related Accounts" for more information.

9.16 Confidential Reporting of AML Non-Compliance

Employees will promptly report any violations of the firm's AML compliance program to the AML Officer, unless the violations implicate the AML Officer, in which case the employee shall report to the firm's CCO or other senior leadership. Alpine believes that compliance with the AML policies and procedures set forth herein are of paramount importance and must be facilitated by the firm. All employee reports concerning AML violations will be kept confidential and no employee ramifications will result from its strict adherence.

9.17 Penalties for Non-Compliance with Alpine Policy or BSA, USA PATRIOT ACT Or Other AML Rules and Regulations

An employee may be deemed to be facilitating or participating in money laundering by engaging in a transaction with a customer (accept a deposit, arrange a withdrawal, effect a trade, *etc.*) when he or she is aware of, or willfully ignores, the fact that the customer is engaged in illegal activities.

Participation in a money laundering scheme or the knowing receipt of proceeds from criminal activities is a crime. Alpine and its employees are subject to severe criminal, civil, and regulatory penalties if they facilitate or participate in money laundering activities. Violations by employees may result in internal disciplinary action, up to and including, termination.

9.18 Additional Risk Areas

Rules/Resources: FinCEN advisory on shell companies: http://www.fincen.gov/AdvisoryOnShells_FINAL.pdf

Alpine has reviewed areas of its business to identify potential money laundering risks that may not be covered in the procedures described above. Other potential risk areas of risk include shell companies as enumerated below.

Shell companies can represent a potential money laundering risk. Most shell companies are formed for legitimate business reasons, but some have been used for illicit purposes.

"Shell company" refers to non-publicly traded corporations, limited liability companies (LLCs), and trusts that typically have no physical presence (other than a mailing address) and generate little or no independent economic value. Legitimate purposes including holding stock or intangible assets of another business entity (such as subsidiary company shares) but are not engaged in active business operations or facilitating domestic and cross-border currency and asset transfers and corporate mergers. Some shell companies have become common tools for money laundering and other financial crimes, primarily because they are easy and inexpensive to form and operate, and ownership and transactional information can be concealed from regulatory and law enforcement authorities. Most states do not collect or require disclosure of ownership information at the formation stage or after (i.e., shell companies can obscure company structure, ownership, and activities), thus, there is little transparency to enable Alpine to understand with whom they are dealing.

Agents that act as intermediaries or nominee incorporation services (NIS) can play a central role in creating, maintaining, and supporting shell companies. Some agents and NIS firms also provide individuals and businesses with nominee services that preserve the anonymity of underlying officers, directors, and stockholders.

Some risk indicators of shell companies potentially engaged in money laundering are:

- An inability to obtain (through Internet searches, commercial database searches, or direct inquiries to the company's foreign correspondent bank) information necessary to identify originators or beneficiaries of wire transfers.
- A foreign correspondent bank exceeds the anticipated volume projected in its client profile for wire transfers in a given period or an individual company exhibits a high amount of sporadic activity that is inconsistent with normal business patterns.
- Payments have no stated purpose, do not reference goods or services, or identify only a contract or service number.
- Goods or services of the company do not match the company's profile based on information previously provided.
- Transacting businesses share the same address, provide only a registered agent's address, or raise other address-related inconsistencies.
- An unusually large number and variety of beneficiaries receive wire transfers from one company.
- Frequent involvement of beneficiaries located in high-risk, offshore financial centers.
- Multiple high-value payments or transfers between shell companies with no apparent legitimate business purpose.

Additional procedures to address this area may include, but not be limited to, the following:

- Checking accounts and owners (if information is available) against OFAC restrictions (applies to all accounts)
- Obtaining information about underlying owners

- Obtaining assurances from the shell company representative that principals have been screened

9.19 Identity Theft Prevention Program (FTC FACT Act Red Flags Rule)

[SEC Securities Exchange Act of 1934 Regulation S-ID; Fair and Accurate Credit Transactions Act (FACT Act) Section 114 and 315; FINRA Regulatory Notice 08-69; FINRA Red Flags Rule web site: http://www.finra.org/Industry/Issues/CustomerInformationProtection/p118480; Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation: http://www.govcollect.org/files/Appendix%20A%20to%20Part%20681.pdf]

Responsibility	• AML Officer or designee
Resources	• New account information • Order records • Transaction information about cash or security transfers • Information reported by employees • Information from third party providers, customers, victims of identity theft, law enforcement agencie or others about potential identity theft
Frequency	• When new accounts are opened • Questionable account addresses changes • Ongoing - review of order records and transaction information • As received - employee information • As required - when a third party is engaged, confirm third party providers have identity theft prograr procedures which may be included in an affirmation in the third party's contract with Alpine • Annually - review of controls and procedures • Obtain senior management approval for any material changes to the program and any material changes to the policy • As needed - update program and provide revisions to senior management for review and approval of material changes. Non-material changes to the Policy will not require senior management approval. • If directed by the CEO, provide revised procedures to the Board or Board committee • Annually - report to CEO • Annually (or more frequently) - provide training for employees

Action	• Establish and maintain the Identity Theft Program
	  ○ Provide initial Program and subsequent material changes to the Board, a Board Committee or CEO (if no Board exists) for review and approval
	  ○ Review controls and procedures annually as part of the annual testing described in the chapter *SUPERVISORY SYSTEM, PROCEDURES AND CONTROLS*
	• Conduct reviews of orders and transactions to identify red flags
	• When red flags are identified, take corrective action which may include:
	  ○ Consultation with the RR and/or supervisor
	  ○ Monitoring the account
	  ○ Contacting the customer
	  ○ Changing passwords, security codes, or other security devices that permit access to an account
	  ○ Reopening an account with another account number
	  ○ Not opening a new account
	  ○ Closing an existing account
	  ○ Filing a Suspicious Activity Report
	  ○ Notifying law enforcement
	  ○ Taking no action if warranted
	• Conduct other reviews which may include:
	  ○ Periodic use of Internet search engines to identify web sites using Alpine's or an RR's nam

	○ Review online advertising to identify web sites for unauthorized links to promote stock fraud or that appear to be illegitimate • If Alpine's or an RR's identity is being used in a scam, take action which may include notifying regulators and the FBI, lodging a complaint at www.ftc.gov, and if it involves email solicitation or spoofing, forwarding email to spam@uce.gov • If a customer's account has been compromised, take action (described in a section that follows) • Include Identity Theft Prevention Program in the annual report to CEO (see the chapter *SUPERVISORY SYSTEM, PROCEDURES AND CONTROLS*), reporting: ○ Effectiveness of the policies and procedures in addressing the risk of identity theft ○ Third party provider arrangements ○ Significant incidents involving identity theft and management's response ○ Recommendations for material changes to the Program • Review third party providers for adequacy of identity theft programs ○ Contractually require them to have policies and procedures to detect Red Flags included in firm policies and report them to Alpine and/or take appropriate steps of their own to prevent/mitigate identity theft • Training: ○ Include identity theft in AML training ○ Develop training, identify target employees, and administer training
Record	• Policies and procedures and revisions • Reviews of orders and transactions with record of action taken • Red flags identified and record of action taken • Annual testing of procedures (see *SUPERVISORY SYSTEM, PROCEDURES AND CONTROLS*) • Annual report to CEO (see *SUPERVISORY SYSTEM, PROCEDURES AND CONTROLS*) • Confirmation that third party providers have adequate ITPPs and include in the contracts with third parties • Records of training including subjects included, date, who administered and who attended

Transactions Act (FACT Act) Section 114 and 315; FINRA Regulatory Notice 08-69; FINRA Red Flags Rule web site: http://www.finra.org/Industry/Issues/CustomerInformationProtection/p118480; Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation: http://www.govcollect.org/files/Appendix%20A%20to%20Part%20681.pdf

9.19.1 Identity Theft Prevention Program Firm Policy

Rules/Resources: 16 C.F.R. § 681.1(d)

Our firm's policy is to protect our customers and their accounts from identity theft and to comply with the FTC's Red Flags Rule. We will do this by developing and implementing this written Identify Theft Prevention Program (ITPP), which is appropriate to our size and complexity, as well as the nature and scope of our activities. This ITPP addresses 1) identifying relevant identity theft Red Flags for our firm, 2) detecting those Red Flags, 3) responding appropriately to any that are detected to prevent and mitigate identity theft, and 4) updating our ITPP periodically to reflect changes in risks.

Our identity theft policies, procedures and internal controls will be reviewed and updated periodically to ensure they account for changes both in regulations and in our business.

9.19.2 ITPP Approval and Administration

Rules/Resources: 16 C.F.R. § 681.1(e) and Appendix A, Section VI.(a)

Alpine's AML Officer is the designated identity theft prevention officer and is responsible for the oversight, development, implementation and administration (including staff training and oversight of third party service providers of ITTP services) of this ITPP.

Alpine's Executive Committee will review and approve this ITPP whenever there are material modifications to the policy.

9.19.3 Relationship to Other Firm Programs

Rules/Resources: 16 C.F.R. § 681.1, Appendix A, Section I

We have reviewed other policies, procedures and plans required by regulations regarding the protection of our customer information, including our policies and procedures under Regulation S-P, and our Customer Identification Program (CIP) and red flags detection under our Anti-Money Laundering (AML) Program in the formulation of this ITPP, and modified either them or this ITPP to minimize inconsistencies and duplicative efforts.

9.19.4 Identifying Relevant Red Flags

Rules/Resources: 16 C.F.R. § 681.1(d)(2)(i) and Appendix A, Section II

To identify relevant identity theft Red Flags, our firm assessed these risk factors: 1) the types of covered accounts it offers, 2) the methods it provides to open or access these accounts, and 3) previous experience with identity theft. Our firm also considered the sources of Red Flags, including identity theft incidents our firm has experienced, changing identity theft techniques our firm thinks likely to occur, and applicable supervisory guidance. In addition, we considered Red Flags from the following five categories (and the 26 numbered examples under them) from Supplement A to Appendix A of the FTC's Red Flags Rule, as they fit our situation: 1) alerts, notifications or warnings from a credit reporting agency; 2) suspicious documents; 3) suspicious personal identifying information; 4) suspicious account activity; and 5) notices from other sources. We understand that some of these categories and examples may not be relevant to our firm and some may be relevant only when combined or considered with other indicators of identity theft. We also understand that the examples are not exhaustive or a mandatory checklist, but a way to help our firm think through relevant red flags in the context of our business. Based on this review of the risk factors, sources, and FTC examples of red flags, we have identified our firm's Red Flags, which are contained the first column ("Red Flag") of the attached "Red Flag Identification and Detection Grid" ("Grid").

9.19.5 Detecting Red Flags

Rules/Resources: 16 C.F.R. § 681.1(d)(2)(ii) and Appendix A, Section III

We have reviewed our covered accounts, how we open and maintain them, and how to detect Red Flags that may have occurred in them. Our detection of those Red Flags is based on our methods of getting information about applicants and verifying it under our CIP of our AML policies and procedures, authenticating customers who access the accounts, and monitoring transactions and change of address requests. For opening covered accounts, that can include getting identifying information about and verifying the identity of the person opening the account by using the firm's CIP. For existing covered accounts, it can include authenticating customers, monitoring transactions, and verifying the validity of changes of address. Based on this review, we have included in the second column ("Detecting the Red Flag") of the attached Grid how we will detect each of our firm's identified Red Flags.

9.19.6 Preventing and Mitigating Identity Theft

We have reviewed our covered accounts, how we open and allow access to them, and our previous experience with identity theft, as well as new methods of identity theft we have seen or foresee as likely to occur. Based on this and our review of the FTC's identity theft rules and its suggested responses to mitigate identity theft, as well as other sources, we have developed our procedures below to respond to detected identity theft Red Flags.

9.19.6.1 Procedures to Prevent and Mitigate Identity Theft

Rules/Resources: 16 C.F.R. □ 681.1(d)(iii) and Appendix A, Section IV

When we have been notified of a Red Flag or our detection procedures show evidence of a Red Flag, we will take the steps outlined below, as appropriate to the type and seriousness of the threat:

Applicants. For Red Flags raised by someone applying for an account:

1. Review the application. We will review the applicant's information collected for our CIP under our AML Program (e.g., name, date of birth, address, and an identification number such as a Social Security Number or Taxpayer Identification Number).
2. Get government identification. If the applicant is applying in person, we will also check a current government-issued identification card, such as a driver's license or passport.
3. Seek additional verification. If the potential risk of identity theft indicated by the Red Flag is probable or large in impact, we may also verify the person's identity through non-documentary CIP methods, including:
    a. Contacting the customer
    b. Independently verifying the customer's information by comparing it with information from a credit reporting agency, public database or other source such as a data broker or the Social Security Number Death Master File.
    c. Checking references with other affiliated financial institutions, or
    d. Obtaining a financial statement.
4. Deny the application. If we find that the applicant is using an identity other than his or her own, we will deny the account.
5. Report. If we find that the applicant is using an identity other than his or her own, we will report it to appropriate local and state law enforcement; where organized or wide spread crime is suspected, the FBI or Secret Service; and if mail is involved, the US Postal Inspector. We may also, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," report it to FINRA, the SEC and State regulatory authorities.
6. Notification. If we determine personally identifiable information has been accessed, we will prepare any specific notice to customers or other required notice under state law.

Access seekers. For Red Flags raised by someone seeking to access an existing customer's account:

1. Watch. We will monitor, limit, or temporarily suspend activity in the account until the situation is resolved.
2. Check with the customer. We will contact the customer using our CIP information for them, describe what we have found and verify with them that there has been an attempt at identify theft or partner with the correspondent firm if it involves one of their direct customers.
3. Heightened risk. We will determine if there is a particular reason that makes it easier for an intruder to seek access, such as a customer's lost wallet, mail theft, a data security incident, or the customer's giving account information to an imposter pretending to represent the firm or to a fraudulent web site.
4. Check similar accounts. We will review similar accounts the firm has to see if there have been attempts to access them without authorization.
5. Collect incident information. For a serious threat of unauthorized account access we may, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," collect if available:
    a. Correspondent firm iinformation, if an introducing brokerage firm
    b. Firm Firm contact name and telephone number
    c. Dates and times of activity
    d. Securities involved (name and symbol)
    e. Details of trades or unexecuted orders
    f. Details of any wire transfer activity
    g. Customer accounts affected by the activity, including name and account number, and
    h. Whether the customer will be reimbursed and by whom.

6. Report. If we find unauthorized account access, we will report it to appropriate local and state law enforcement; where organized or wide spread crime is suspected, the FBI or Secret Service; and if mail is involved, the US Postal Inspector. We may also, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," report it to FINRA; the SEC; and State regulatory authorities.
7. Notification. If we determine personally identifiable information has been accessed that results in a foreseeable risk for identity theft, we will prepare any specific notice to customers and to others where required by law or regulation.
8. Review our insurance policy. Since insurance policies may require timely notice or prior consent for any settlement, we will review our insurance policy to ensure that our response to a data breach does not limit or eliminate our insurance coverage.
9. Assist the customer. We will work with our customers to minimize the impact of identity theft by taking the following actions, as applicable:

    a. Offering to change the password, security codes or other ways to access the threatened account;
    b. Offering to close the account;
    c. Offering to reopen the account with a new account number;
    d. Not collecting on the account or selling it to a debt collector; and
    e. Instructing the customer to go to the FTC Identity Theft Web Site to learn what steps to take to recover from identity theft, including filing a complaint using its online complaint form, calling the FTC's Identity Theft Hotline 1-877-ID-THEFT (438-4338), TTY 1-866-653-4261, or writing to Identity Theft Clearinghouse, FTC, 6000 Pennsylvania Avenue, NW, Washington, DC 20580.

9.19.7 Alpine Employees Reporting Obligations

Identity thieves use someone's personal identifying information to open new accounts and misuse existing accounts. Alpine has established an Identity Theft Prevention Program (ITPP) to help detect and prevent identity theft. Many elements of detecting or preventing identity theft utilize similar techniques to that of the anti-money laundering (AML) requirements included within these policies.

The ITPP is based on identifying "red flags" which may indicate an occurrence of identity theft. ***It is the responsibility of all employees to be attentive and alert to the red flags and report to the AML Officer or designeeany new or existing customers who may be engaged in violations of anti-money laundering regulations, identity theft or who have reported an instance of identity theft.***

For a list of potential identity theft red flags, refer to the section titled "*Red Flag Identification and Detection Grid*" located in the ***Identity Theft Prevention Program (FTC Fact Act Red Flags Rule)*** section.

9.19.8 Service Providers

Rules/Resources: 16 C.F.R. § 681.1(e)(4) and Appendix A, Section VI.(c)

We may use other service providers in connection with our covered accounts. In the event we utilize other service providers, we have a process to confirm that any other service provider that performs activities in connection with our covered accounts, especially other service providers that are not otherwise regulated, comply with reasonable policies and procedures designed to detect, prevent and mitigate identity theft by contractually requiring them to have policies and procedures to detect Red Flags and report detected Red Flags to us or take appropriate steps of their own to prevent or mitigate the identify theft.

9.19.9 Internal Compliance Reporting

Rules/Resources: 16 C.F.R. § 681.1, Appendix A, Section VI.(b)

Firm staff responsible for developing, implementing and administering our ITPP will report at least annually to our Executive Committee on compliance with the FTC's Red Flags Rule. The report will address the effectiveness of our ITPP in addressing the risk of identity theft in connection with covered account openings,

existing accounts, service provider arrangements, significant incidents involving identity theft and management's response and recommendations for material changes to our ITPP.

9.19.10 Updates and Annual Review

Our firm will update this plan whenever we have a material change to our operations, structure, business or location or to those of our clearing firm, or when we experience either a material identity theft from a covered account, or a series of related material identity thefts from one or more covered accounts. Our firm will also follow new ways that identities can be compromised and evaluate the risk they pose for our firm. In addition, our firm will review this ITPP annually, to modify it for any changes in our operations, structure, business, or location or substantive changes to our relationship with our clearing firm.

Rule: 16 C.F.R. § 681.1 (d)(2)(iv) and Appendix A, Sections V. and VI. (a) & (b).

9.19.11 Red Flag Identification and Detection Grid

Red Flag	Detecting the Red Flag
Category: Suspicious Documents	
1. Identification presented looks altered or forged.	Our staff who deal with customers and their supervisors will scrutinize identification presented in person to make sure it is not altered or forged. Note: Alpine is not required to take steps to determine whether the document has been validly issued. We may rely on government issued identification as verification of a customer's identity.
2. The identification presenter does not look like the identification's photograph or physical description.	Our staff who deal with customers and their supervisors will ensure that the photograph and the physical description on the identification match the person presenting it.
3. Information on the identification differs from what the identification presenter is saying.	Our staff who deal with customers and their supervisors will ensure that the identification and the statements of the person presenting it are consistent.
4. Information on the identification does not match other information our firm has on file for the presenter, like the original account application, signature card or a recent check.	Our staff who deal with customers and their supervisors will ensure that the identification presented is matched to known information we have on file for the account.
5. The application looks like it has been altered, forged or torn up and reassembled.	Our staff who deal with customers and their supervisors will scrutinize each application to make sure it is not altered, forged, or torn up and reassembled.
Category: Suspicious Personal Identifying Information	
6. Inconsistencies exist between the information presented and other things we know about the presenter or can find out by checking readily available external sources	If we receive a consumer credit report, they will check to see if the addresses on the application and the consumer report match.
7. Inconsistencies exist in the information that the customer gives us	Our staff will check personal identifying information presented to

	us to make sure that it is internally consistent
8. Personal identifying information presented has been used on an account our firm knows was fraudulent.	Our staff will compare the information presented with addresses and phone numbers on accounts or applications we found or were reported were fraudulent
9. Personal identifying information presented suggests fraud, such as an address that is fictitious, a mail drop, or a prison; or a phone number is invalid, or is for a pager or answering service.	Our staff may validate the information presented when opening an account by looking up addresses on the Internet to ensure they are real and not for a mail drop or a prison, and may call the phone numbers given to ensure they are valid and not for pagers or answering services.
10. The SSN presented was used by someone else opening an account or other customers.	Our staff may compare the SSNs presented to see if they were given by others opening accounts or other customers.
11. The address or telephone number presented has been used by many other people opening accounts or other customers.	Our staff may compare address and telephone number information to see if they were used by other applicants and customers.
12. A person who omits required information on an application or other form does not provide it when told it is incomplete.	Our staff will track when applicants or customers have not responded to requests for required information and will follow up with the applicants or customers to determine why they have not responded.
13. Inconsistencies exist between what is presented and what our firm has on file.	Our staff will verify key items from the data presented with information we have on file.
14. A person making an account application or seeking access cannot provide authenticating information beyond what would be found in a wallet (or consumer credit report, if applicable) or cannot answer a challenge question.	Our staff may authenticate identities for existing customers by asking challenge questions that have been prearranged with the customer and for applicants or customers by asking questions that require information beyond what is readily available from a wallet or a consumer credit report.
Category: Suspicious Account Activity	
15. Soon after our firm gets a change of address request for an account, we are asked to add additional access means (such as debit cards or checks) or authorized users for the account.	We will verify change of address requests by sending a notice of the change to the old addresses so the customer will learn of any unauthorized changes and can notify us.
16. A new account exhibits fraud patterns, such as where a first payment is not made or only the first payment is made, or the use of securities easily converted into cash, if margin is permitted.	We will review new account activity to ensure that payments are made, and that credit is primarily used for securities easily converted into cash, if margin is permitted.
17. An account develops new patterns of activity, such as nonpayment inconsistent with prior	We will review our accounts periodic basis and look for suspicious new

history, a material increase in credit use, or a material change in spending patterns, or electronic funds transfers (if applicable).	patterns of activity such as nonpayment, a large increase in credit use, or changes in spending patterns or electronic fund transfers (if applicable).
18. An account that is inactive for a long time is suddenly used again.	We will review our accounts on a periodic basis to see if long inactive accounts become very active, if the circumstances suggest that the activity may be potentially suspicious in nature.
19. Mail our firm sends to a customer is returned repeatedly as undeliverable even though the account remains active.	We will note any returned mail for an account andmay check the account's activity, if the circumstances suggest that the activity may be potentially suspicious in nature.
20. We learn that a customer is not getting his or her paper account statements.	We will record on the account any report that the customer is not receiving paper statements and may investigate, if the circumstances suggest that the activity may be potentially suspicious in nature
21. We are notified that there are unauthorized charges or transactions to the account.	We will verify if the notification is legitimate and involves a firm account, and then investigate the report.
Category: Notice From Other Sources	
22. We are told that an account has been opened or used fraudulently by a customer, an identity theft victim, or law enforcement.	We will verify that the notification is legitimate and involves a firm account, and then investigate the report.
23. We learn that unauthorized access to the customer's personal information took place or became likely due to data loss (e.g., loss of wallet, birth certificate, or laptop), leakage, or breach.	We will contact the customer to learn the details of the unauthorized access to determine if other steps are warranted.

9.20 Senior Manager Approval

The AML Officer or designee will seek and obtain written approval from the senior management team for any and all material changes to Alpine's AML policy. Changes that do not result in a material change to the policy will not require approval. Please refer to the section titled "AML Officer" for more information.

10 INSIDER TRADING

[Insider Trading and Securities Fraud Enforcement Act of 1988; '34 Act 10b-5; FINRA Notice to Members 89-5]

Responsibility	• Trading department supervisor
Resources	• Daily Transaction Report • Employee transactions (see the section *Employee, Employee-Related and Proprietary Trading*)